المجلة العراقية للعلوم الإحصائية (25) 2013
عدد خاص بوقائع المؤتمر العلمي السادس لكلية علوم الحاسوب والرياضيات
ص ص[441-455]

اخفاء المعلومات عبر الهاتف النقال باستخدام البلوتوث

د.أحمد سامي نوري* شذى عبد المنعم بكر**

الخلاصة

نظراً للتطور الهائل لوسائل الاتصال وتبادل المعلومات أصبحت الخصوصية الشخصية عرضة للانتهاك بسهولة أكبر من ذي قبل، لهذا ظهرت الحاجة إلى اعتماد تقنية أكثر تطوراً وأكثر سريةً وحفاظا على المعلومات فأُستعملت الكتابة المغطاة. فالكتابة المغطاة هي علم إخفاء بيانات سرية مهمة في ناقل غير مؤذٍ على نحو يخفي وجود البيانات المخفية بدون إثارة الشبهة بهدف إبقاء الاتصال بين الطرفين المتصلين سويا. ويُعدُّ الهاتف النقال أحد وسائل الاتصال اللاسلكي المتطور اذ تطور هذا الجهاز بسرعة مذهلة. ففضلاً عن كونه وسيلة اتصال صوتي، تعددت استعمالاته ووظائفه، لتجعل منه جهاز كمبيوتر لحفظ معلومات كثيرة ومتعددة، تصفح مواقع الأنترنيت، آلة تصوير، ، أداة للعب والتسلية، ..الخ.

في هذا البحث قُدمت طريقة جديدة للإخفاء لتضمين المعلومات السرية (صوت) في صور ذات احجام مختلفة كغطاء لتلك المعلومات السرية ومن دون حصول أي تشويه يجذب الانتباه. اما عملية اختيار المواقع للاخفاء فقد تمت عن طريق توليد الارقام عشوائيا باستخدام مفتاح خاص، والذي يستخدم ايضاً في عملية الاسترجاع. كما اعتمد العمل على تقنية البلوتوث في عمليات الارسال. وأثبتت التجارب تفوق الطرائق من خلال مقاييس الأداء (MSE, PSNR,NC) ، اذ أظهرت النتائج مدى فاعليتها ومتانتها، علماً اللغة التي استخدمت في التنفيذ كانت لغة J2ME.

Information Hiding Over Mobile using Bluetooth

ABSTRACT

Due to the evolution of massive means of communication and the exchange of information has become personal privacy vulnerable to abuse more easily than ever before, so there is a need to adopt the technology more sophisticated and more secret and preserve the information,

*استاذ مساعد / قسم علوم الحاسوب/ كلية علوم الحاسوب والرياضيات/ جامعة الموصل

**باحثة / قسم علوم الحاسوب / كلية علوم الحاسوب والرياضيات/ جامعة الموصل

تاريخ استلام البحث 2013/10/10 ـــــــــــــــــــــــ تأريخ القبول 2013/11/21

Steganography was used. Steganography is a science hide confidential data in the carrier task inoffensive manner embeds the existence of hidden data without raising suspicion in order to keep the contact between the two callers confidential. The mobile phone is considered as wireless means of communication as the evolution of this amazing device quickly. In addition to being a means of voice communication, there were many uses and functions, to make it a computer for saving a lot of and multiple information, surf the Internet web sites, a camera and a tool to play and entertainment, .. etc.

This paper provided new method to hide using Steganography to include secret information (voice) in images with different sizes as a cover for such secret information without getting any distortion brings attention. The operation of selecting sites to hide it has by generating random numbers using a private key, which is also used in the recovery operation. It also adopted the Bluetooth transmission operations. Experiments proved the modalities through performance measures (MSE, PSNR, NC). As the results showed the effectiveness and durability. The implementation was done using J2ME language.

1- المقدمة

ويعد الهاتف النقال من أهم الأدوات التكنولوجية في الوقت الراهن وأكثرها ملازمة لحياتنا اليومية، وقد رافق هذا الانتشار تعدد استخدامات هذا الجهاز، فلم يعد الهاتف النقال مقتصرا على إجراء المكالمات الهاتفية وإرسال الرسائل النصية بل تعدى الأمر ذلك بكثير لتجعل منه جهاز كمبيوتر لحفظ معلومات كثيرة ومتعددة، وتصفح مواقع الإنترنيت، واستخدام الوسائط المتعددة، وآلة تصوير تضاهي الكاميرات الرقمية من حيث نقاء الصورة ووضوحها، وأداة استقبال البريد الصوتي، والدخول إلى البريد الالكتروني والحسابات المصرفية وتحويل الأموال، واحد وسائل الإعلام[1].

وأصبحت خدمات الهاتف النقال الأكثر أهمية من بين وسائل الاتصال كما هو الحال مع الانترنت بسبب المحاسن المتوافرة فيه والمتمثلة بتوافرها العالي واستقلاليتها عن الزمان والمكان، لذلك ظهرت الحاجة الى حماية المعلومات المتوافرة في هذا الجهاز من التغيير والتلاعب ولاسيما مع هذا التطور الواسع والسريع لشبكة الهاتف النقال وشمولها لانواع مختلفة من المعلومات مثل : الرسائل والصور والفيديو، فأدى ذلك لاستخدام وسيلة أخرى في مجال تطوير أمنية البيانات وهي علم إخفاء المعلوماتInformation Hiding والغاية منه ليس فقط منع المتطفلين من معرفة المعلومات

المخفية بل لإزالة الشك أصلا بوجود هذه المعلومات والشيء المميز في تقنية الإخفاء أنها تواكب التقنيات الحديثة ويمكن استخدامها في جميع الوسائط المتعددة من صور ونصوص وصوت وفيديو.

قدم البحث تصميم تطبيقين في الهاتف النقال أولهماتصميم تطبيق تضمين الصوت، وثانيهما: استرجاع الصوت، وقد تم استخدام تقنية البلوتوث بوصفها وسيلة لنقل البيانات، والاجهزة التي تم فيها تنفيذ التطبيقين اعلاه مصنعة من شركة نوكيا (N8, C6-01) وتعمل بنظام تشغيل سمبيان.

2- الدراسات السابقة

شهدت بدايات العقد الأخير من القرن الماضي ظهور طليعة البحوث حول الكتابة المخفية الرقمية، اذ اقترح الباحث (Mohammad Shirali 2007) ارسال عنوان موقع الصورة المحملة بالبيانات السرية عبر SMS بدلاً من الارسال المباشر لبيانات الصورة، فيقوم المستلم بتحميل الصورة من الموقع واسترجاع البيانات المضمنة اعتماداً على مفتاح سري متفق عليه بين الطرفين[2]. واستخدم (Ritesh Pratap Singh 2010) وآخرون خدمة MMS التي يوفرها الهاتف النقال لارسال الصورة المضمنة بالبيانات السرية، اذ اعتمدوا على طريقة الطيف المنتشر Spread Spectrum بالاخفاء والتي تعمل على انتشار البيانات في نطاق اوسع ضمن صورة الغطاء مما يصعب اكتشاف البيانات المضمنة من قبل المتطفل، ان الطريقة المقترحة إعتمدت على الصور الرمادية فقط وكانت النتائج جيدة [3]. وفي العام نفسه قدم الباحث (M.I.Khalil) فكرة مقترحة لاخفاء الصوت داخل صورة ملونة، بتجزئته الى جزءين الاول خاص بالـ Header للملف الصوتي وتضمينه داخل المستوى G للصورة الغطاء، اما الثاني فهو بقية مكونات الملف الصوتي الذي اعتمد في تضمينه فكرة ابدال الـ bit الاقل اهمية (LSB) لكن باسلوب جديد وهو استخدام بوابة XOR المنطقية مع بيانات الصورة الغطاء واعتماد نواتجها لتخزن في المستويين R,B من الصورة[4].

وفي عام 2012 قدم الباحث (Chandrakant Badgaiyan) وآخرون بحثاً تُخفى فيه صور بامتدادات مختلفة عن طريق الاضافة وليس الطمر ضمن تطبيق يعمل في الهاتف النقال مثل الرسام والالعاب، ان هذا التطبيق يعمل بصورة طبيعية الى ان يتم ادخال المفتاح السري والذي هو عبارة عن حدث معين Specific event، عندها يتوقف التطبيق وتعرض الصورة المخفية [5]. كما شهدت السنة نفسها بحثاً آخر حيث قدم الباحث (Hameed AbdulKareem 2012)

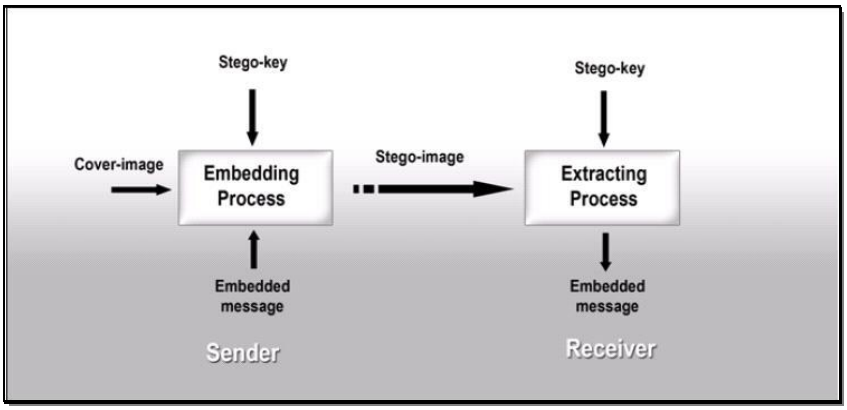
وآخرون في عملهم المقترح طريقةً تستخدم لاخفاء صوت معين داخل صورة ملونة، و الطريقة المقترحة تعتمد على تخزين ثنائيات الصوت في الطبقة الثالثة LSB3 من ثنائيات الصورة بدلاً من الطبقة الاولى LSB1، وذلك لزيادة متانة بيانات الصوت داخل الغطاء، فضلاً عن استعمال مفتاح سري والذي اعطى مزيداً من الحماية، وكانت النتائج حسنة[6] .

3- إخفاء المعلومات

إن إخفاء المعلومات يعني تضمين معلومات في معلومات أخرى ظاهرها لا يدعو إلى الشك ولا يلفت الانتباه، والهدف المتحقق بعملية الاخفاء هو عدم إثارة اي شك بوجود بيانات مخفية لذلك يعد عاملا مهماً في إضفاء حماية وأمناً على المعلومات، ويعتمد على مبدأ ان الرسالة المرسلة تكون غير مرئية لأي شخص بواسطة اخفائها في محتويات الوسائط المتعددة بتغيير بعض المكونات غير الضرورية في الملف الغطاء، وبذلك يبقى محتواها حكراً على الجهات ذات العلاقة التي تكون على دراية بكيفية استرجاع هذا المحتوى [7][8].

إن إطار عمل اغلب طرائق الإخفاء يوضحها الشكل (1) وتتضمن ما ياتي [9]:

- ❖ تحليل عناصر ملف الغطاء cover، وتهيئتها لاستقبال البيانات السرية.
- ❖ تحليل عناصر الرسالة السرية المطلوب تضمينها (إخفاء بياناتها)embedded message.
- ❖ تطبيق الخوارزمية المناسبة للإخفاء ويكون استخدام المفتاح اختيارياً لإنتاج ما يسمى stego-message .
- ❖ إرسال ملف الغطاء المتضمن للبيانات السرية من المرسل .
- ❖ استلام ملف الغطاء من الطرف المقصود الإرسال إليه.
- ❖ تحليل عناصر ملف الغطاء واستخراج عناصر الملف المضمّن وفق نفس الخوارزمية المتّبعة في الإخفاء.
- ❖ تجميع البيانات للحصول على الملف المضمّن كاملاً.



الشكل (1) النموذج العام لنظام التغطية [10]

4- الشبكات اللاسلكية

تعد الشبكات اللاسلكية نظاماً مرناً لتوصيل البيانات ونستخدم كامتداد او كبديل للشبكات السلكية، حيث تقوم هذه الشبكات ببث المعلومات عن طريق امواج الراديو Radio Frequency وقد انتشر هذا النوع من الشبكات وازداد أعداد المستخدمين لخدماتها. وتعتبر الشبكات اللاسلكية حلا أمثل لتجنب الصعاب التي قد يتطلبها تمديد أسلاك الشبكات السلكية، وأهم ما تمتاز به هو القدرة على الوصول للأماكن التي لا تتوافر بها توصيلات شبكية[11]. إن وسائط النقل اللاسلكية متعددة وأخذت بالتطور شيئاً فشيئا ومن هذه الوسائط هو البلوتوث Bluetooth ، فتقنية البلوتوث مبنية على المواصفات القياسية (IEEE 802.15.1 Institute of Electrical and Electronics Engineers) وتعرف بأنها اتصالات لاسلكية قصيرة المدى صممت لاستبدال الكابلات المستخدمة في الشبكات السلكية لتعمل على ربط كل من الأجهزة المحمولة أو الأجهزة الثابتة، وتعمل على الطيف الترددي 2.4GHz، ومن أهم مميزاته[12]:

1. أنه قصير المدى حيث يصل مداه الى 10 أمتار.
2. قوة مقاومته للضوضاء والإشوا ات التي تتداخل معه فهي لا تؤثر فيه.
3. تكلفته قليلة اذ إن تصميمه سهلو غير مكلف.
4. سهولة العمل به فهو لا يتطلب أية إعدادات خاصة، ويمتاز بمستوى عال من التوافق بين الأجهزة، فالأجهزة التابعة له كل منها يفهم الآخر من دون أن يضطر المستخدم إلى القيام بأي شيء أو تغيير أية بروتوكولات عمل.

5- لغة جافا الإصدار المصغر J2ME

في عام (2000) إصدرت شركة (Sun MicroSystem) لغة (Java 2 Micro Edition J2ME)، وصممت هذه اللغة لبرمجة الأجهزة الصغيرة والاستهلاكية ذات الذاكرة المحدودة مع قوة العرض والمعالجة وقد استخدمت على مدى واسع من الأجهزة مثل أجهزة الهواتف النقالة وأجهزة الاستدعاء والأجهزة الكفية[13]. لغة J2ME قسمت الى ثلاثة إجراء رئيسة لكي تُفهم بصورة سلسلة وسهلة هي[14]:

- التشكيلات (Configurations)
- التوصيفات(Profiles)
- واجهات تطبيقات المبرمج (Application Programming Interfaces APIs) الاختيارية

إن هذه الأجزاء الرئيسة في لغة جافا الإصدار المصغر(J2ME) تزود المبرمج بمعلومات عن واجهات تطبيقات المبرمج(APIs) ومعلومات عن مختلف أنواع الأجهزة.

6- الطريقة المقترحة

تشتمل عملية التضمين الخطوات الآتية كما موضح بالشكل (2):

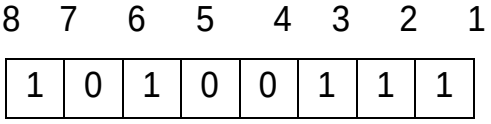
- اختيار الرسالة السرية (Secret message) والمتمثلة بملف صوتي مخزون في الهاتف النقال أو يُستعمل برنامج المسجل لإدخال الصوت المراد إخفاوه.
- اختيار الصورة الغطاء، والعمل على تحليلها إلى ثلاثة مستويات (R, G, B).
- تُحوّل بيانات الصوت السري إلى مصفوفة ذات بعد واحد وبالتمثيل الثنائي(binary bits).
- تُحوّل بيانات المستويات (R, G, B) لصورة الغطاء إلى مصفوفة ذات بعد واحد وبالتمثيل الثنائي(binary bits) لتبدأ بعدها عملية تضمين بيانات الصوت السري.
- يُولّد المفتاح الخاص بعملية الإخفاء عن طريق استخدام دالة توليد الأرقام العشوائية، اذ يُستفاد من التاريخ الموجود في الهاتف النقال (تسلسل اليوم ضمن أيام الأسبوع) وجعله الادخال (بذرة) لدالة توليد الأرقام العشوائية.
- يتم بعد اختيار موقع Byte عشوائي من الصورة الغطاء، تطبيق(XOR operation) بين بت الإخفاء و الخلية الثنائية من بيانات النص السري ليُعتمد في الخلية الثنائية الأولى b1 من بيانات الصورة الغطاء، إن بت الإخفاء يُحتسب على النحو الآتي:

في البدء توضع القيمة 0 في الخلية الثنائية الأولى للـ Byte المستخلص من بيانات الغطاء، بعدها تجرى عملية تقسيم الـByte إلى جزءين:

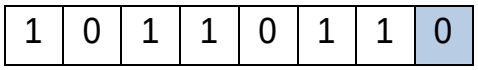
الجزء الأول الخلايا الثنائية الأربعة الأولى (b1,b2,b3,b4)

الجزء الثاني الخلايا الثنائية الأربعة الأخيرة (b5,b6,b7,b8)

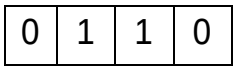
ثم تُطبق عملية الجمع بين الجزءين فالبت الفائض carry يمثل بت الإخفاء، كما موضح في المثال الآتي:

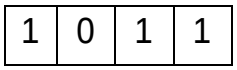


جعل قيمة b1 مساوية للصفر

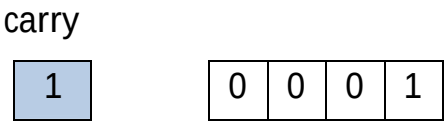


تقسيم الـ byte إلى جزءين





جمع الجزءين



- بعد الانتهاء من عملية التضمين توضع العلامة # للدلالة على نهاية بيانات الصوت ، يُحوّل من النظام الثنائي إلى النوع RGB للحصول على الـ Stego_image.

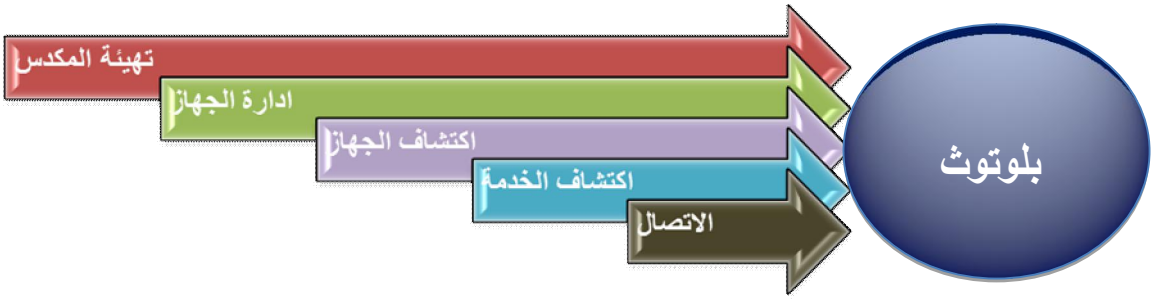
اما عملية الاسترجاع فتشتمل على الخطوات الاتية والشكل (3) يوضح خطوات استرجاع الصوت :

- يقوم المستلم بتحليل الـ Stego_Image وفصلها إلى ثلاثة مستويات (R, G, B)، ثم تُحوّل الى مصفوفة ذات بعد واحد وبالتمثيل الثنائي (binary bits) لتبدأ بعدها عملية استخراج بيانات الصورة السرية.
- يُولّد المفتاح السري الخاص بعملية الإسترجاع بنفس الطريقة المتبعة في عملية التضمين.
- تقترح الطريقة بعد اختيار موقع byte عشوائي من الـ Stego_Image، بتطبيق (XOR operation) بين بت الإخفاء والخلية الثنائية الاولى b1 من بيانات الـ Stego_Image ليُوضع في مصفوفة البيانات السرية، إن بت الإخفاء يُحستب على النحو الاتي:

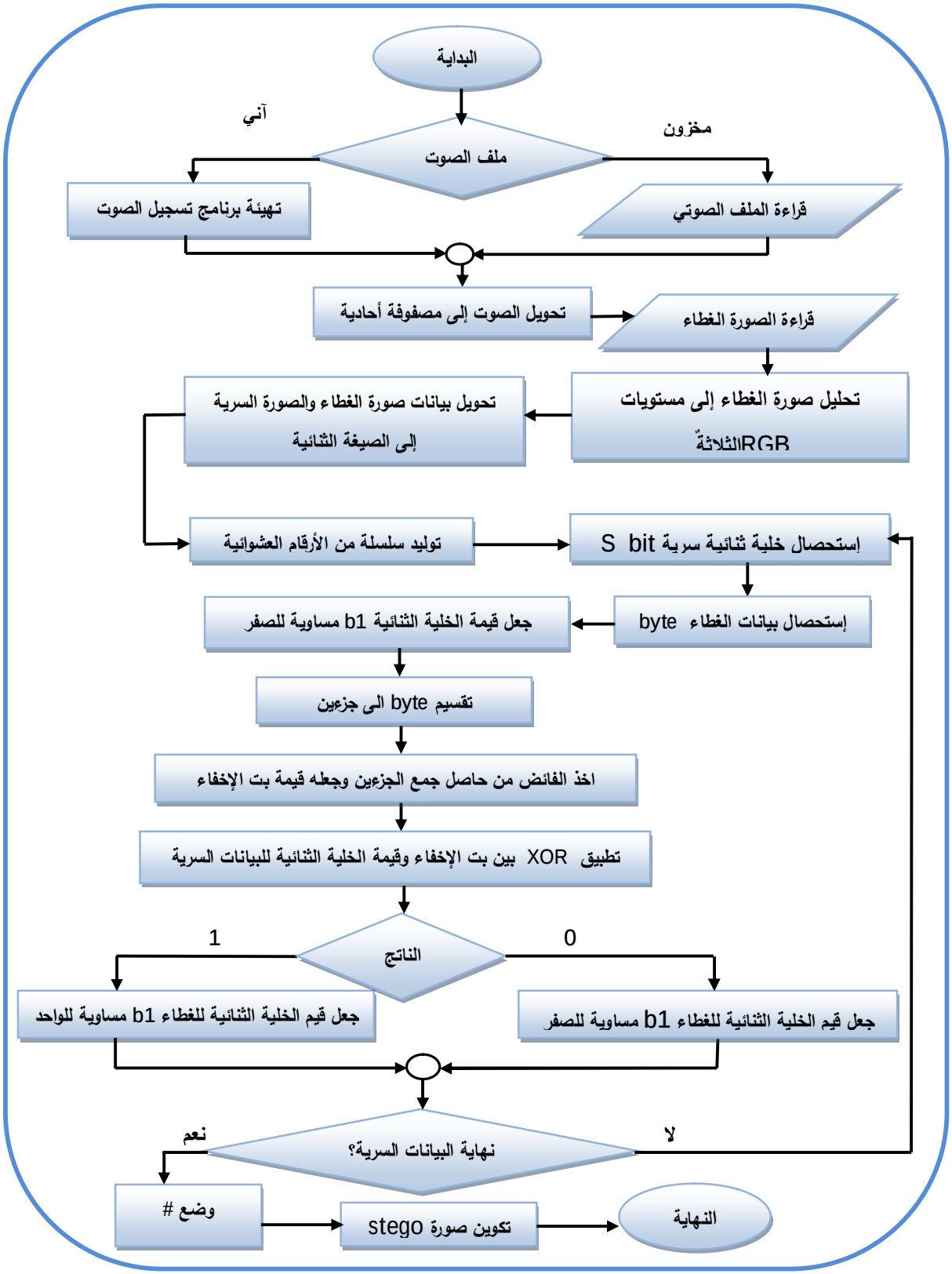
في البدء توضع القيمة 0 في الخلية الثنائية الأولى للـ Byte المستخلص من بيانات الـ Stego_Image، بعدها تجرى عملية تقسيم الـByte إلى جزءين: الجزء الأول الخلايا الثنائية الأربعة الأُول (b1,b2,b3,b4)، الجزء الثاني الخلايا الثنائية الأربعة الأخيرة (b5,b6,b7,b8)، ثم تُطبق عملية الجمع بين الجزءين فالبت الفائض carry يمثل بت الإخفاء، بحيث إن المحصلة النهائية للقيم المخزونة تكون عبارة عن مصفوفة ذات بعد واحد التي تمثل البيانات السرية التي تُحول من النظام الثنائي الى RGB لإعادة تكوين الصورة المسترجعة.

7- آلية تطبيق تقنية البلوتوث

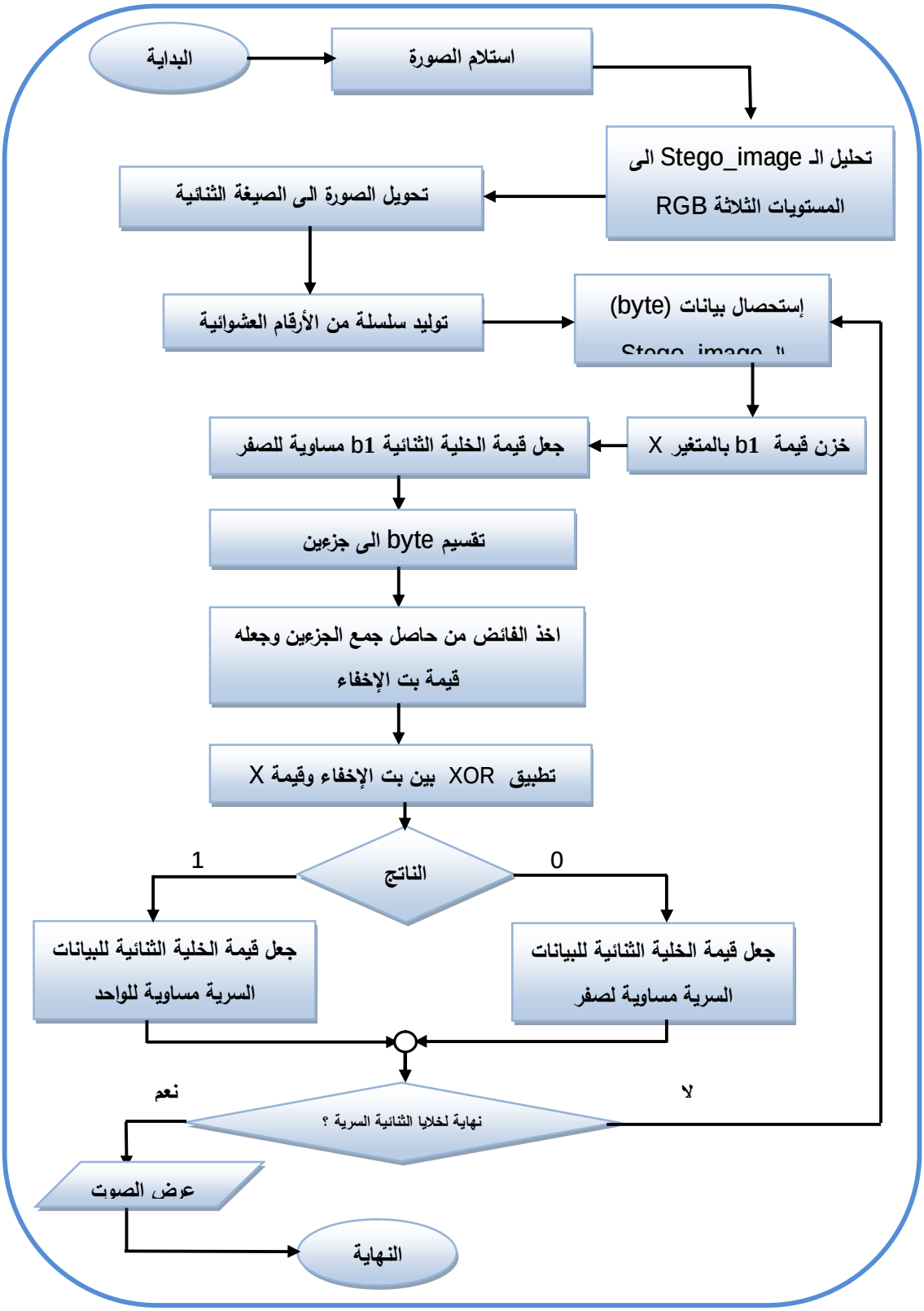
إن المراحل التي يمر بها تطبيق تقنية البلوتوث موضحة بالشكل (4)و هي:



الشكل (4) مراحل تهيئة البلوتوث



الشكل (2) مخطط انسيابي لتضمين الصوت



الشكل (3) مخطط انسيابي لاسترجاع الصوت

1.تهيئة المكدس

مكدس البلوتوث هو المسؤول عن السيطرة على جهاز البلوتوث، لذلك يُهيئ مكدس البلوتوث كخطوة أولى تهدف للحصول على استعداد الجهاز للاتصال اللاسلكي[15] .

1. إدارة الجهاز

يقدم الصنف LocalDevice إمكانية الوصول الى جهاز البلوتوث المحلي، يُومن الكائن من صنف LocalDevice طرائق للحصول على المعلومات عن الجهاز، بما في ذلك عنوان و الجهاز واسمه ويمثل بوابة لبدء عمليات البحث المختلفة [16]. والمقطع البرمجي الذي يمثل هذه العملية:

```
//retrieve the local Bluetooth device
LocalDevice local = LocalDevice.getLocalDevice()
//retrieve the Bluetooth address and name of the local device
String address = local.getBluetoothAddress()
String name = local.getFriendlyName()
```

2. اكتشاف الجهاز

إن استخدام الصنف DiscoveryAgent يوفر الخدمات اللازمة لاكتشاف الأجهزة، وإرجاعها للتطبيق حالما يُعثر عليها، فباستخدام DiscoveryAgent.startInquiry يبدأ بطلب استعلام، فتقوم الأجهزة المحيطة به بالاستجابة لطلب الاستعلام هذا، اذ تستجيب هذه الأجهزة بعنوان البلوتوث الذي لديها وصنف سجل الجهاز[14]. يوجد نوعان من طلبات الاستعلام هما[15] :

- طلب الاستعلام العام(General Inquiry Access Code GIAC) الذي يُستخدم لإيجاد أجهزة البلوتوث في المنطقة المحيطة.
- طلب الاستعلام الخاص(Limited Inquiry Access Code LIAC) وعمله إيجاد جميع الأجهزة في المنطقة المحيطة التي لديها قابلية البحث عنها لمدة محددة من الوقت.

تشكل الواجهة DiscoveryListener جزءًا آخر من عمليتي البحث عن الأجهزة والبحث عن الخدمة، كما يُصرّح عن الواجهة DiscoveryListener ضمن التطبيق لاستقبال الأجهزة وسجلات الخدمة حالما يُعثر عليها.

```
// retrieve the discovery agent
DiscoveryAgent agent = local.getDiscoveryAgent( )
//place the device in inquiry mode
boolean complete = agent.startInquiry ( )
```

3. اكتشاف الخدمة

إن اكتشاف الخدمة يشبه إلى حد كبير اكتشاف الجهاز، اذ يوفر DiscoveryAgent الامكانية لاكتشاف الخدمات المتوفرة على الجهاز، ثم يقوم بإنشاء سجل الخدمة الذي يصف الخدمة المقدمة [15].

```
ServiceRecord sr = local.getRecord(service)
```

الاتصال

إن Bluetooth API توفر الآليات التي تسمح بالاتصال مع اية خدمة باستخدام بروتوكولات معينة مثل RFCOMMو OBEX [14]. في النظام المقترح أُستخدم البرتوكول RFCOMM في ارسال البيانات واستقبالها، اذ تعتمد عملية الاتصال على مبدأ الخادم والعميل (Server & Client) وحسب المهام الآتية لكل طرف [17]:

اولاً: جهة الخادم

- بناء URL التي تشير إلى كيفية الاتصال بالخدمة، وتخزينها في سجل الخدمة.
- جعل سجل الخدمة متوفر للعميل.
- قبول الاتصال من العميل.
- إرسال البيانات واستقبالها من وإلى العميل.

ثانياً: جهة العميل

تهيئة اكتشاف الخدمة لاسترجاع سجل الخدمة.

- بناء URL التي تشير إلى كيفية الاتصال بالخدمة باستخدام سجل الخدمة.
- فتح اتصال مع الخادم.
- إرسال البيانات واستقبالها من وإلى الخادم.

8-النتائج والمناقشة

تم تطبيق الطريقة المقترحة على صور بابعاد مختلفة (256x256) و (512x512) و(480 x 640) موضحة بالشكل (5)، وأعتمدت المقاييس التالية لإثبات كفاءة الطريقة[18]:

$$PSNR = 10 \log_{10}\left(\frac{255^2}{MSE}\right) \text{..... .... (1)}$$

$$MSE = \frac{1}{mn}\sum_{x=0}^{m-1}\sum_{y=0}^{n-1} steg\_im(x,y) - cover\_im(x,y) \text{..... .... (2)}$$

$$NC = \sum_{x=0}^{m-1}\sum_{y=0}^{n-1} steg\_im(x,y) * cover\_im(x,y) / \sum_{x=0}^{m-1}\sum_{y=0}^{n-1}((cover\_im(x,y))^2 \text{.....(3)}$$

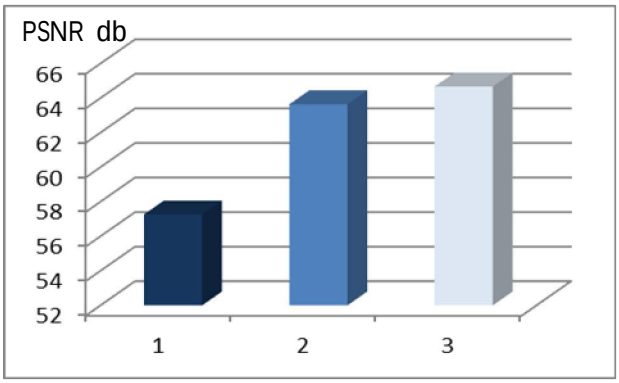
حيث ان: Steg_im تمثل صورة الاخفاء و cover_imتمثل صورة الغطاء و m , n ابعاد الصورة

حيث نلحظ من الجدول (1) والخاص بعملية التنفيذ ان قيم PSNR تزداد مع زيادة حجم الغطاء اي ان العلاقة طردية، وان NC اعطى اعلى النتائج والتي جاءت مطابقة لمقاييس الجودة والكفاءة المطلوبة. كما ان الطريقة حققت نسبة عالية في عدم القدرة على تمييز الصورة الغطاء عن Steg_im او بمعنى اخر عدم القدرة على الاكتشاف حتى عندما تكون كمية البيانات السرية كبيرة.

الشكل (5) نماذج لتطبيق االطريقة المقترحة

الجدول (1) نتائج تنفيذ الطريقة المقترحة على أنواع من الصور

Image	Pixels	MSE	PSNR	NC
Image1	256x256	0.122	57.2672	1
Image2	512x512	0.2816	63.6437	1
Image3	640 x 480	0.0222	64.6672	1



الشكل(6) مقارنة بين قيم PSNR لتضمين ملف صوتي في صور بابعاد مختلفة

9- الاستنتاجات

ان العمل مع الهاتف النقال اكثر صعوبة بسبب اختلاف الاجهزة، ومن خلال التطبيق العملي تم التوصل إلى:

- استحدثت في هذا البحث طريقة جديدة لتصميم نظام إخفاء والإفادة من الامكانيات التي يوفرها الهاتف النقال فهو فضلاًعن انه وسيلة اتصال، فانه يوفر نهجاً جديداً بامكانية توفير الرسالة السرية انياً، وعن طريق التطبيق العملي للنظام تبين مدى فاعلية طريقة الإخفاء المُتبعة، اذ ان هذه الطريقة من نوع (blind) التي باعتمادها يُمكن استخراج المعلومات السرية دون الحاجة الى وجود الغطاء الأصلي.
- ان الطريقة المعتمدة في توليد المفتاح السري اعطى سرية أكبر للخوارزمية.
- ان استخدام الصور الملتقطة بكاميرة الهاتف النقال واعتمادها غطاءً حاملاً للبيانات السرية حقق درجة عالية من الأمنية، وذلك لتوفيرها القدرة على إبعاد الشبهات كونها صعبة المقارنة لإنعدام الاصل لدى المتطفل.
- اعتمادا على مواصفات الهاتف النقال يمكن زيادة كمية البيانات المضمنة مع المحافظة على جودة الصورة.
- إن العمل المُقترح لا يؤثر في جودة الصورة، وبعبارة أخرى يمكن القول إنه لا يوجد أي تشويه يمكن ملاحظته، وهذا ما اثبتته مقاييس الجودة والكفاءة التي استُعملت

المصادر

[1] Wong, K.Y., (2010), "Cell Phones as Mobile Computing Devices", Macao Polytechnic Institute, IEEE IT Pro Computer Society.

[2] Shirali-Shahreza, M., (2007), "Improving Mobile Banking Security Using Steganography", Fourth International Conference on Information Technology(ITNG'07), IEEE, p. 885-887.

[3] Singh, R. P., Khan M. A., Khan, M., and Singh N., (2010), "Spread Spectrum Image Steganography in Multimedia Messaging Service of Mobile Phones", International Journal of Electronics Engineering, pp. 365–369.

[4] Khalil, M.I, (2011), "Image Steganography: Hiding Short Audio within Digital Images", JCSandT, Vol. 11, No. 2.

[5] Badgaiyan, C., Dewangan, A.K., Pandey, B.K., Yeulkar, K. and Sinha, K.K., (2012), "A New Steganography Technique Image Hiding in Mobile Application", International Journal of Advanced Computer and Mathematical Sciences, Vol. 3, Issue4.

[6] Younis,H. A., Jalil, A. J. and Abbood, Z. A., (2012), "Steganography System to Hide a Sound File in a Color Image", J.Thi-Qar Sci. Vol.3 3.

[7] Indra, M., Reddy, S., Reddy, M. P., and Reddy, K. S., (2012), "Different Medias of Steganography- An Emerging Field of Network Security", International Journal of Computer Science and Information Technologies, Vol. 3 , No. 2 , pp. 3517-3522.

ابراهيم، نجلاء بديع و نوري، احمد سامي و طه، دوجان بشير، (2010)، " تشفير وإخفاء المعلومات في ملفات الإنترنت[8] HTMLو XML"، مجلة الرافدين لعلوم الحاســبات والرياضيات، المجلد 7، العدد 1.

الحمامي، علاء حسين ومحمد علاء، (2008)، "إخفاء المعلومات: الكتابة المخفية والعلامــة المائية "، إثراء للنشر[9] والتوزيع، الشارقة

[10] Goel, P., (2008), "Data Hiding in Digital Images : A Steganographic Paradigm", Master's Thesis, Indian Institute of Technology– Kharagpur.

[11] Jabbar, A.I., and Ayoob, S. A., (2012), "A new Model of a Wireless AD- HOC Network with Sub-Layer Mac Using Simevents Tools", Al-Rafidain Engineering, Vol.20, No. 5.

[12] Wang, H., (2001), "Overview of Bluetooth technology", University Pennsylvania, Philadelphia.

[13] Muchow, J., (2002), "CORE J2me Technology & MIDP", Sun Microsystems, Inc. , USA .

[14] Li, S. and Knudsen, J., (2005), "Beginning J2ME From Novice To Professional", 3rd Edition , Apress , USA .

[15] Williams, B., (2002), "Java Applications for a Bluetooth Platform", The University of Queensland, Australia.

[16] Buyya, R., Selvi S. T. and Chu. X. ,(2009), "Object-Oriented Programming with Java", First Edition, McGraw-Hill Publishing .

[17] Thompson, T., Kline, P. and Kumar, C. B., (2008), "Bluetooth Application Programming With the javaTM APIs Essentials Edition", Morgan Kaufmann Publishers, USA.

[18] Batra. N. and Kaushik. P., "Data Hiding in Color Images Using Modified Quantization Table", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume 1, Issue 8, 2012.