GLM for Image Steganography Technique

Ahmed S. Nori **Noor N. Ahmed** **Thana Gh. Ahmed**
ahmed.s.nori@uomosul.edu.iq
College of Computer Science and Mathematics
University of Mosul, Mosul, Iraq

Received on: 15/10/2012 **Accepted on: 30/01/2013**

ABSTRACT

An improvement to a Steganography method for hiding data using Gray Level Images is proposed in this paper. The method is an improvement over earlier method named Least Significant Bit (LSB). This method uses the 5th, and 6th bits of pixel value for insertion and retrieval of message by using the same bits of pixel value.

The idea here, deals with images in different sizes and extensions (BMP, JPG, PNG) for obtaining better results and more efficient than its original one (LSB). The selection of pixel locations is done by using the pseudo random number generator, Which is uses the same key for insertion as well as retrieval of process.

The experiments show the Superiority of the new idea through using the performance measures (PSNR, BER, NC).

Keywords: GLM, LSB, BMP, JPG, PNG.

GLM لتحسين تقنية الإخفاء بالصور

أحمد سامي نوري **نور نظير أحمد** **ثناء غانم أحمد**
كلية علوم الحاسوب والرياضيات
جامعة الموصل، الموصل، العراق

الملخص

يعرض هذا البحث تقنية محسنة لتطبيق الإخفاء (إخفاء المعلومات) في صور المستوى الرمادي. والتحسين هنا هو لطريقة الإخفاء باستخدام bit الأقل أهمية Least Significant Bit (LSB). إذ تم اختيار أرقام bit 5 و 6 من قيمة pixel للإدخال واسترجاع الرسالة باستخدام bit نفسه من قيمة pixel .

التطبيق هنا، كان مع الصور ذات الأحجام والامتدادات المختلفة (BMP، JPG، PNG) من أجل الحصول على نتائج أفضل وأكثر كفاءة من تقنية (LSB) الأصلية. أما عملية اختيار المواقع للإخفاء (مواقع pixel) فقد تمت عن طريق توليد الأرقام عشوائيا باستخدام مفتاح خاص، والذي يستخدم أيضاً في عملية الاسترجاع. أثبتت التجارب تفوق الفكرة الجديدة من خلال مقاييس الأداء (BER، NC، PSNR).

الكلمات المفتاحية: صور المستوى الرمادي، البت الاقل اهمية، BMP، JPG، PNG .

1. المقدمة

يخلط كثيراً من المبتدئين في العلم المختص بحماية وأمن المعلومات بين علم التشفير وعلم إخفاء المعلومات، معتقدين أن كلا المصطلحين يعطي المعنى نفسه، في حين أن كل مصطلح منهما يغطي علماً خاصاً

من علوم أمن المعلومات. تهدف تقنية إخفاء المعلومات إلى الإخفاء التام لوجود هذه المعلومات عن طريق إخفائها داخل معلومات أخرى ليست بتلك الأهمية مع الحرص التام على عدم تأثر المعلومات المستخدمة للإخفاء بحقيقة كونها حاملة للمعلومات المخفية وذلك لتجنب احتمالية الكشف عن وجود المعلومات المخفاة تحت هذه المعلومات. باستخدام هذه الطريقة تقل نسبة الكشف عن المعلومات والعبث بها بنسبة كبيرة؛ لأنه إن كان المهاجم لا يعلم بوجود هذه المعلومات أصلاً فكيف باستطاعته العبث بها والاستفادة منها؟[3]

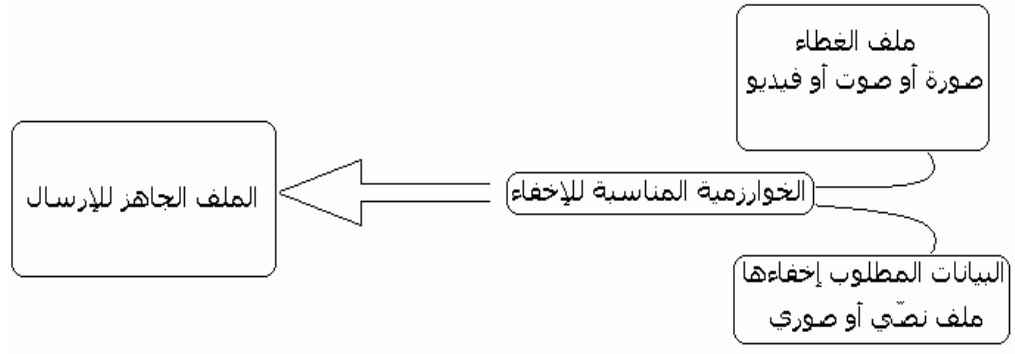
2. علم الإخفاء

يأتي أصل مصطلح علم إخفاء المعلومات (Steganography) من الكلمتين الإغريقيتين: stegos والتي تعني السقف أو الغطاء وgraphia والتي تعني الكتابة. ويعرف علم إخفاء المعلومات على أنه إخفاء رسالة ما (بيانات) داخل رسالة أخرى (بيانات أخرى) بهدف إخفاء وجود الرسالة الأولى لهدف محدد. والبيانات المستخدمة في الإخفاء قد تكون عبارة عن ملفات الوسائط المتعددة (multimedia) كالنصوص، الصور، وملفات الصوت أو الفيديو وغيرها. وقد تكون أيضا عبارة عن ملفات تنفيذية للبرامج (executable file). وفي عملية الإخفاء نحتاج إلى توفر عنصرين مهمين لإتمام هذه العملية، الأول هو الرسالة التي نهدف إلى إخفائها والثاني هو الغطاء (cover) المستخدم لإخفاء هذه الرسالة.[4]

3. المبدأ العام لعلم الإخفاء

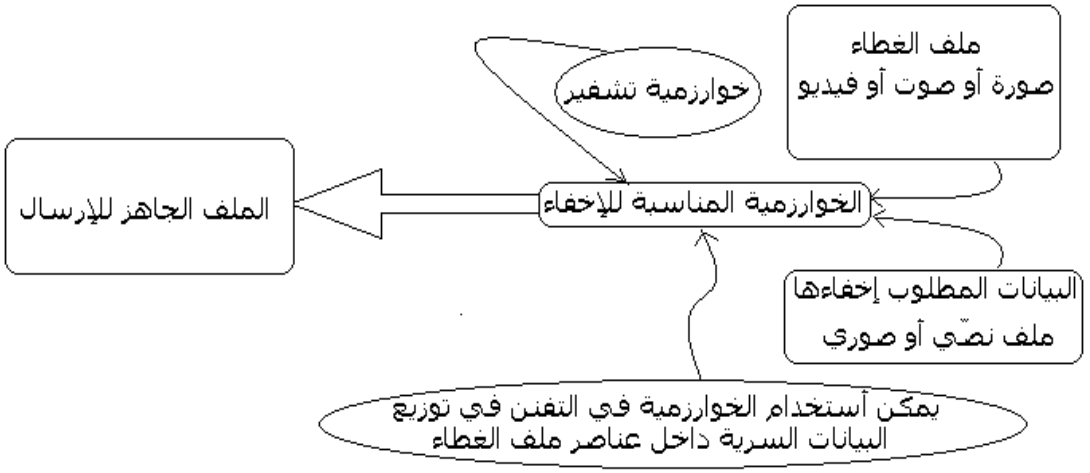
أغلب طرائق علم الإخفاء تتبع المبدأ العام التالي: الأشكال (1) و(2)

1- تحليل عناصر ملف الغطاء، وتحضيرها لاستقبال البيانات السرية.
2- تحليل عناصر الملف المطلوب تضمينه (إخفاء بياناته).
3- تطبيق الخوارزمية المناسبة للإخفاء.
4- إرسال ملف الغطاء المتضمن للبيانات السرية من قبل المرسل.
5- استلام ملف الغطاء من قبل الطرف المقصود الإرسال إليه.
6- تحليل عناصر ملف الغطاء واستخراج عناصر الملف السري وفق نفس الخوارزمية المتّبعة في الإخفاء.
7- تجميع البيانات للحصول على الملف السري كاملاً.



الشكل (1). عملية إخفاء البيانات داخل ملف الغطاء

أن علم التشفير يمكن أن يزيد من قوة العمل، إذ سيصبح من الصعب تحديد وجود إخفاء في الملف المُرسل، ثم يصبح من المعقد فك النص المخفي المشفر، وهنالك طرائق عديدة من أساليب التشفير.



الشكل (2). عملية إخفاء البيانات المشفرة داخل ملف الغطاء

هل تغيير bit واحد من كل byte يكفي لإخفاء بيانات كاملة لنص أو لصورة؟ أن الصور من نوع BMP والمستخدمة بوصفها ملف غطاء لكبر حجمها ولكثرة البيانات التي تجمعها والصور السرية هي من نوع JPG أو مثيلاتها، فحجم صورة BMP يبلغ إضعاف حجم الصورة السرية نوع JPG، وبالتالي فبإمكان صورة صغيرة من نوع BMP أن تخفي في بياناتها ملفاً نصّياً لأكثر من صفحتين.

إن خوارزمية bit الأقل أهمية هي من أقوى الخوارزميات الموجود في علم الإخفاء، وأكثرها شيوعا والتي تترك أثراً بسيطاً جداً في ملف الغطاء إذا ما أُحسنت برمجتها، ويتعسّر على العين البسيطة استكشاف التأثير، وبالتالي يستعصي فك رموزها حاسوبياً إذا ما أُخذ بنظر الاعتبار التفنن في الإخفاء، واستخدام صور غير متوفرة النسخ.[5]
ومن الملاحظ في هذه الطريقة:

1- إذا تم تغيير أول خلية ثنائية من كتلة الصورة الملونة الممثلة بشكل 3-Bytes فان كل نقطة يتم فيها تغيير 3-Bit، لان كل نقطة ممثلة بشكل 3-Bytes وهذا التغيير لن يكون ملاحظا للعين البشرية.
2- عند استخدام الصورة الممثلة 8-Bit فيفضل استخدام الصورة الرمادية، لان التغيير سيكون غير ملحوظاً. [1]

4. أعمال سابقة

في العام (2009) قدمت كل من (فرح باسل احمد وآخرين) فكرة إخفاء باعتماد حماية الملكية في الصور وكانت النتائج جيدة في حينها. [1]

أما كل من (رؤى سامي إسماعيل وآخرون) فقد قدموا في العام (2009) بحثاً عن "تطبيقات العلامة المائية في المجال المكاني" واستطاعوا أن يثبتوا أن العملية أفضل من سابقتها. [2] كما استطاعت (رفل أديب، سالي عبد الجبار) في العام (2010) تقديم "إخفاء المعلومات باستخدام الشبكات العصبية الاصطناعية". [6]

وكذلك (Ravi Saini, Rajkumar Yadav) سنة (2011) قدما طريقة مقترحة من خلال "تقنية جديدة للإخفاء في الصور باستخدام الصور الرمادية". [7]

5. وصف الطريقة المقترحة

في الخوارزمية المقترحة سوف نستخدم bit (5^{th}, 6^{th}) من قيم pixel وكما يلي:

إذا كان الإدخال (قيمة bit السرية) = صفراً

- إذا كانت القيمة العشرية bit (5^{th}, 6^{th}) تساوي 2، 0، إذاً تبقى كما هي.
- إذا كانت القيم العشرية bit (5^{th}, 6^{th}) لا تساوي 2، 0، إذاً يضاف واحد لتلك المواقع.

إذا كان الإدخال (قيمة bit السرية) = واحداً

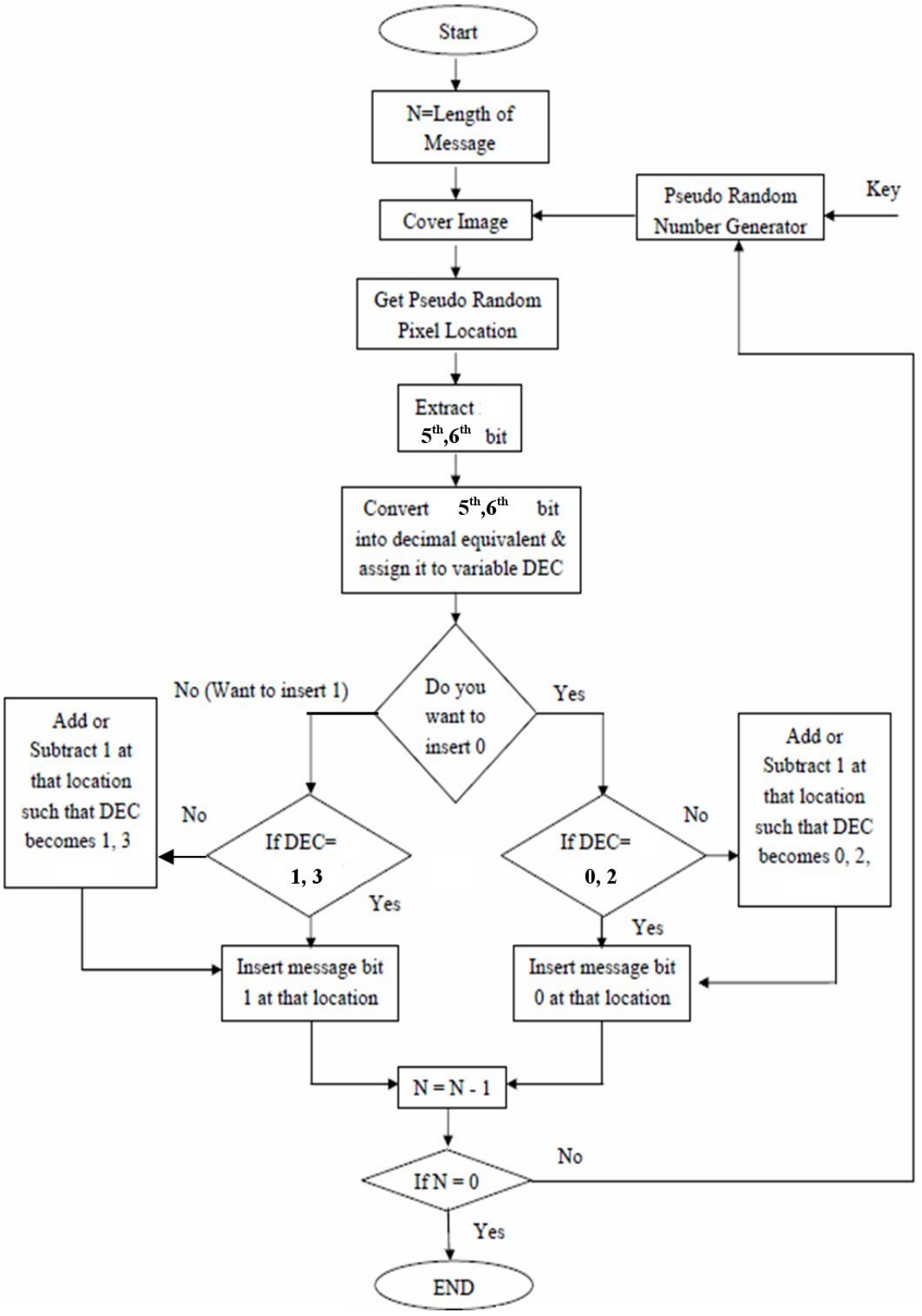
- إذا كانت القيمة العشرية bit (5^{th}, 6^{th}) تساوي 3، 1 إذا تبقى كما هي.
- إذا كانت القيمة العشرية bit (5^{th}, 6^{th}) لا تساوي 3، 1 إذا يضاف واحد لتلك المواقع.

لاسترجاع الرسالة نفحص القيمة العشرية bit (5^{th}, 6^{th})

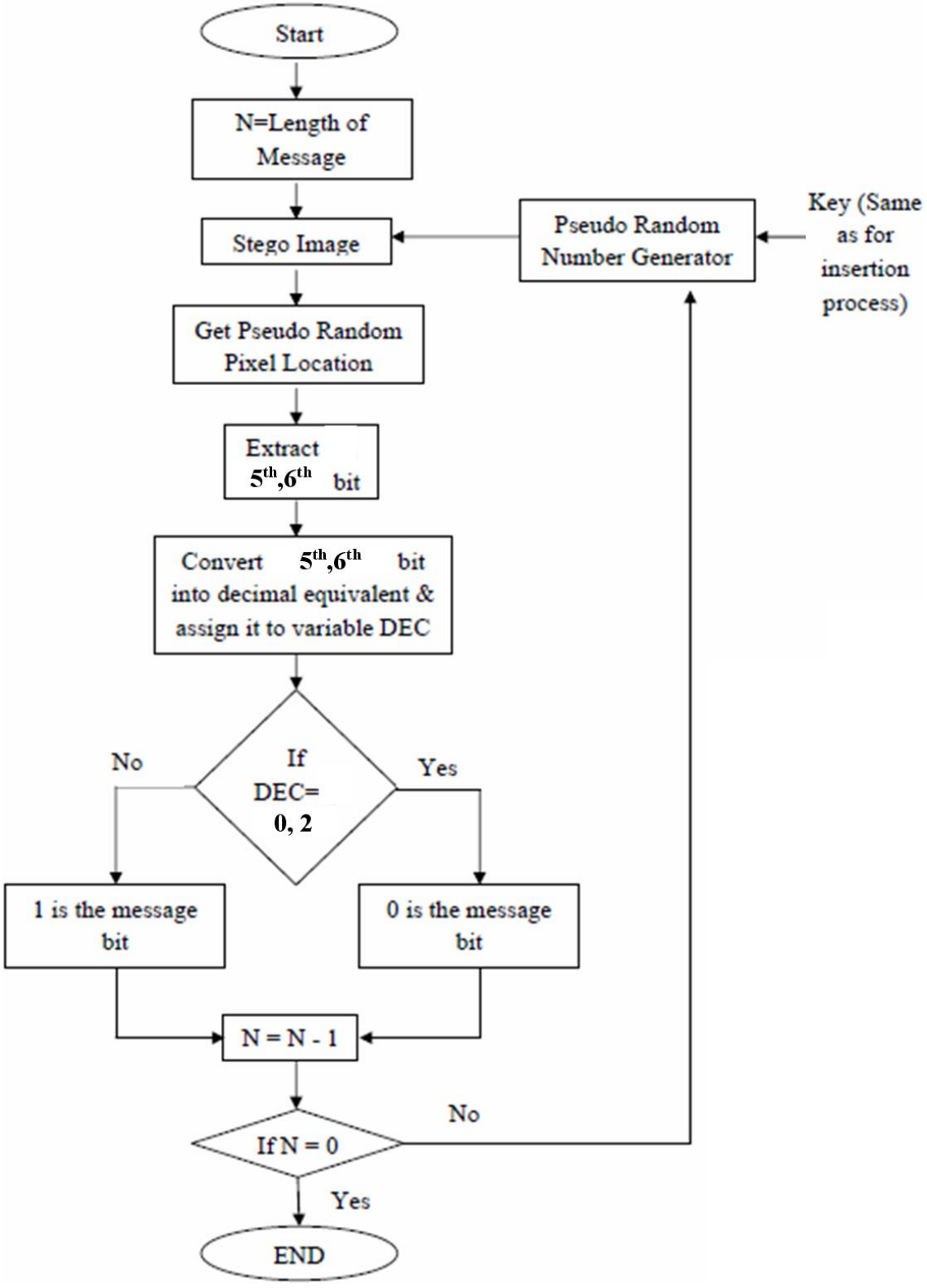
- إذا كانت تساوي 2، 0 فهذا يعني قيمة bit = (0) وإلا فهي = (1)

في هذه الخوارزمية سوف نستخدم bit (5^{th}, 6^{th}) لإدخال واسترجاع الرسالة وذلك لإلغاء المساوئ الموجودة في خوارزمية (LSB) والحصول على أفضل النتائج.

الأشكال (3) و(4) توضح مخطط عملية الإخفاء والاسترجاع على التوالي.



الشكل (3). مخطط انسيابي لعملية الإخفاء



الشكل (4). مخطط انسيابي لعملية الاسترجاع

6. مثال عن الخوارزمية المقترحة

تم اخذ صورة وتحويلها إلى التدرج الرمادي ولنفرض أنها تعطي مجموعة pixel الموضحة بالشكل (5) ولنفرض انه مطلوب إخفاء الرسالة 100101 في هذه الصورة فيتم تحديد مجموعة من المواقع العشوائية الأشكال (6، 7) والتي تمثل المفتاح الذي سيستخدم في الإخفاء والاسترجاع.

الشكل (5).
نموذج لتطبيق الخوارزمية المقترحة

Columns

Rows	1	2	3	4	5	6	7	8	9	10
1	11	15	20	18	33	79	89	84	210	213
2	217	137	25	85	27	23	45	84	71	215
3	21	45	46	90	112	125	118	17	77	81
4	81	64	65	84	29	210	201	245	139	174
5	11	91	71	206	154	109	219	135	31	87
6	41	47	147	98	87	97	35	135	140	104
7	201	215	115	83	53	43	95	10	47	65
8	95	68	35	64	74	46	32	16	86	65
9	23	16	18	85	43	214	201	105	10	101
10	51	47	29	16	84	47	65	35	38	49

الشكل (6). قيم الترددات الرمادية للصورة المقترحة

Columns

Rows	1	2	3	4	5	6	7	8	9	10
1	11	15	20	18	33	79	89	84	210	213
2	217	137	25	85	27	23	45	84	71	215
3	21	45	46	90	112	125	118	17	77	81
4	81	64	65	84	29	210	201	245	139	174
5	11	91	71	206	154	109	219	135	31	87
6	41	47	147	98	87	97	35	135	140	104
7	201	215	115	83	53	43	95	10	47	65
8	95	68	35	64	74	46	32	16	86	65
9	23	16	18	85	43	214	201	105	10	101
10	51	47	29	16	84	47	65	35	38	49

الشكل (7). تحديد المواقع المختارة باستخدام توليد **أرقام عشوائية**

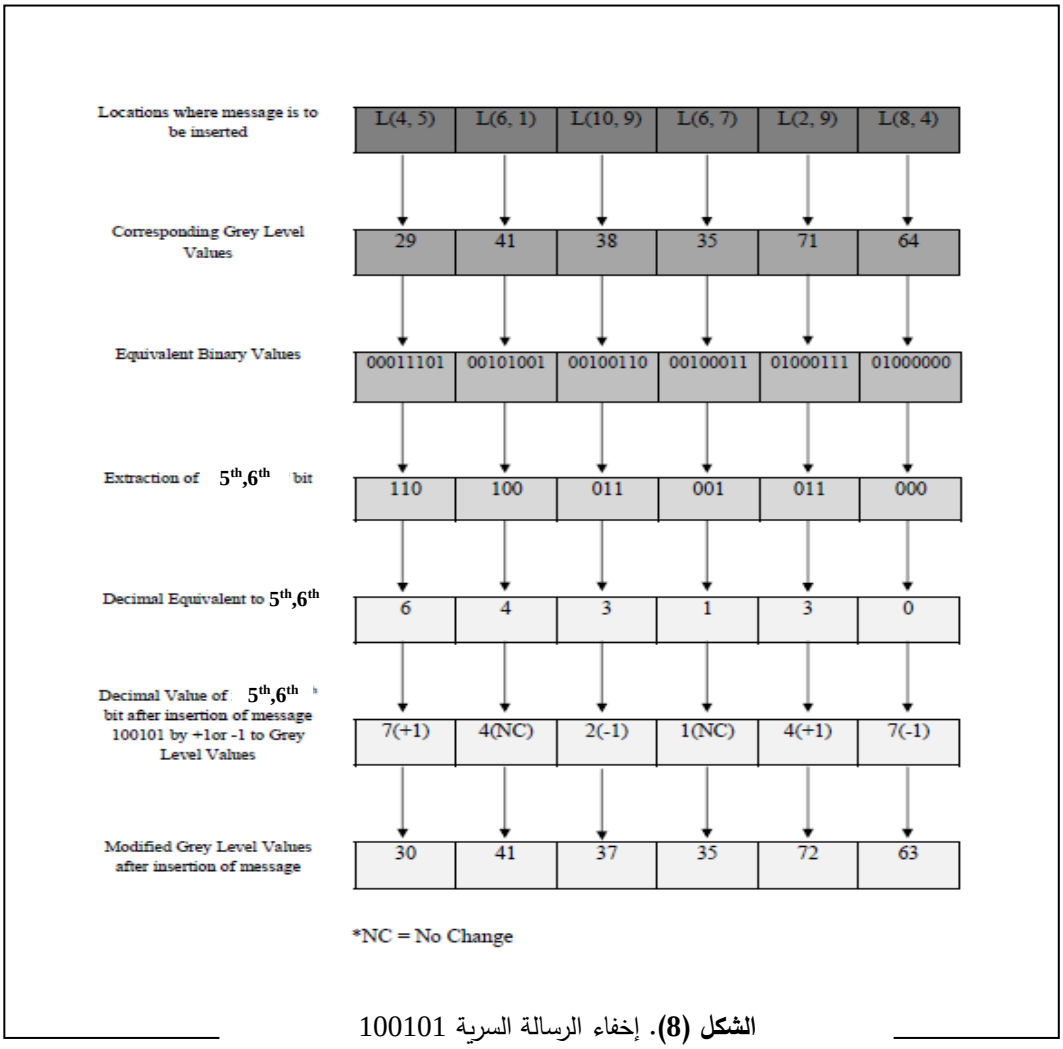
حيث تم تحديد المواقع:

L (4, 5), L (6, 1), L (10, 9), L (6, 7), L (2, 9), L (8, 4)

والتي تمثل الصف والعمود للمواقع وتم الحصول على القيم:

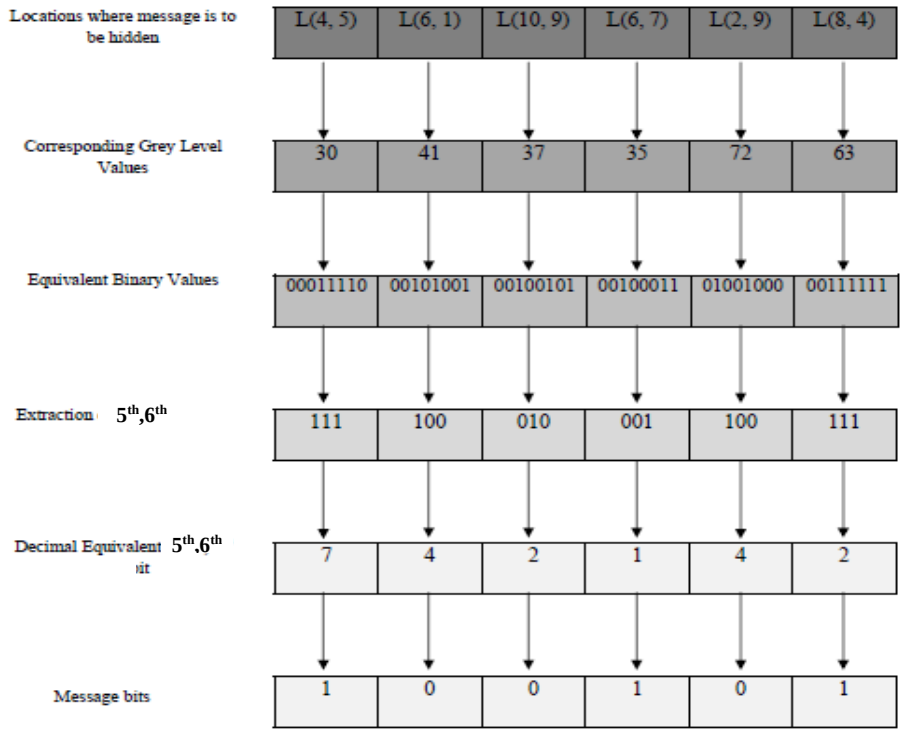
29, 41, 38, 35, 71 and 64.

يمكن توضيح عملية الحشر بالشكل (8).



الشكل (8). إخفاء الرسالة السرية 100101

أما عملية الاسترجاع فيمكن توضيحها بالشكل (9).



الشكل (9). استرجاع الرسالة السرية 100101

تم اعتماد المقاييس التالية لإثبات كفاءة الطريقة المقترحة ...

$$PSNR = 10.\log_{10}\left(\frac{(\text{Max value of Gray level})^2}{MSE}\right) \quad \ldots(1)$$

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

حيث إن:

$steg\_im$: يمثل صورة_الإخفاء، و $cover\_im$: يمثل صورة_الغطاء. m و n : أبعاد الصورة

BER = (no. of wrong bit / no. of original bit) * 100 ...(3)

$$NC = \sum_{x=0}^{m-1}\sum_{y=0}^{n-1} steg\_im(x,y) * cover\_im(x,y) / \sum_{x=0}^{m-1}\sum_{y=0}^{n-1}((cover\_im(x,y))^2 \quad \ldots(4)$$

فيما يأتي ندرج الجدول (1) والخاص بعملية التنفيذ والذي يعطي أفضلية واضحة للطريقة المقترحة على سابقتها.

الجدول (1). نتائج تنفيذ الطريقة المقترحة على أنواع من الصور (BMP، PNG ،JPG)

ت	اسم الصورة	نوع الصورة	حجم الصورة	PSNR	NC	BER
1	Bird	BMP	600*400	66.6523	1	0
2	Boat	JPG	540*320	59.8754	0.9785	0.063
3	Car	BMP	800*600	67.8621	1	0
4	Ship	JPG	720*640	59.9879	0.9854	0.021
5	Butterfly	JPG	760*550	59.8952	0.9821	0.022
6	See	BMP	780*690	64.7397	0.9993	0
7	Eagle	PNG	770*680	63.8794	0.9991	0.003

7. الاستنتاجات

تعد هذه الطريقة أفضل من (LSB) التقليدية للأسباب الآتية:

1- إذا قام المتطفل بتغير bit الأقل أهمية لكل المواقع في صورة الغطاء ففي طريقة LSB فانه لا يمكن استرجاع المخفية.

2- إذا تم تغيير بعض bit الأقل أهمية بسبب الضوضاء فباستخدام طريقتنا في الاسترجاع فان الرسالة المخفية سوف تسترجع بصورة صحيحة وبدون أخطاء.

3- من الجدول أعلاه تبين بان الطريقة المقترحة قد أعطت قيما عالية PSNR واقل ما يمكن بالنسبة BER مما يعني الجودة العالية.

4- إن لغة البرمجة (Matlab) أعطت للعمل دعماً وجهداً مميزاً من ناحية الكفاءة والقدرة على التنفيذ وتوفير الدوال المساعدة.

5- لموضوع الإخفاء أبعاد ومجالات عديدة ومتنوعة تفتح أفاقاً كثيرة للعمل فيه.

المصادر

[1] أحمد، فرح باسل و ندى جزيل ونجلاء طلب، (2009)، "حماية الملكية في الصور"، بحث تخرج، كلية علوم الحاسوب والرياضيات، جامعة الموصل.

[2] إسماعيل، رؤى سامي وعبد القادر، هبة هاني وعلي، شهلة عبد، (2009)، ""تطبيقات العلامة المائية في المجال المكاني"، بحث تخرج، كلية علوم الحاسوب والرياضيات، جامعة الموصل.

[3] الحمامي، علاء حسين ومحمد علاء، (2008)، "إخفاء المعلومات"، إثراء للنشر والتوزيع.

[4] برزنجي، فوزي، (2008)، "فن الاختزال"، جامعة السليمانية.

[5] حسن، زينة محمد ويونس، خليل احمد، (2009)، "الإخفاء في ملفات الانترنيت"، بحث تخرج، كلية علوم الحاسوب والرياضيات، جامعة الموصل.

[6] رفل أديب وسالي عبد الجبار، (2010)، "إخفاء المعلومات باستخدام الشبكات العصبية الاصطناعية"، بحث تخرج، كلية علوم الحاسوب والرياضيات، جامعة الموصل.

[7] RajKumar, Yadav, et al, (2011), "Anew Image Steganography Approach For Information Security Using Gray Level Images In Spatial Domain", International Journal On Computer Science And Engineering (IJCSE), July.