Encrypted and Hiding Information in Digital Images using Wavelet Transformation and LSB Technology

Ahmed Hamed Saleh Al-Badrani

Technical College of Management
Technical Institute, Mosul, Iraq

Received on: 17/09/2012 **Accepted on: 30/01/2013**

ABSTRACT

Hiding information is an effective solution for the protection of copyright and confidentiality to allow a person to send the data in the middle of the cover image to a person without knowing any third party in this transmission, methods of delivering secret messages are very important. This research provides a way to hide data (which is a text file) after is encrypted adoption method (Keyword Mixed Transposition) to produce cipher text is included in Low–High coefficient wavelet transform and get a good quality image and the possibility of recovering fully embedded message and decoded without relying on the original image. Results have applied to the digital images to get inline images to the data with a high correlation coefficient when compared with the original images in addition to that they gave a few differences when calculating measurements(SNR, PSNR, MSE).

Keywords: Encrypted, hiding information, wavelet transformation, and LSB Technology

تشفير وإخفاء المعلومات في الصور الرقمية باستخدام التحويل المويجي وتقنية LSB

أحمد حامد صالح البدراني

الكلية التقنية الإدارية / الموصل

هيئة التعليم التقني، الموصل، العراق

تاريخ استلام البحث: 2012/09/17 **تاريخ قبول البحث: 2013/01/30**

الملخص

إن أخفاء المعلومات هو حل فعال لحماية حقوق الطبع والسرية بحيث تسمح للشخص بإرسال البيانات في وسط غطاء (Cover Image) إلى شخص بدون معرفة أي طرف ثالث بهذا الإرسال، إن طرق تسليم الرسائل السرية مهمة جداً. هذا البحث يقدم طريقة لإخفاء البيانات (والتي هي عبارة عن ملف نصي txt File) بعد إن يتم تشفير النص باعتماد طريقة (Keyword Mixed Transposition) لإنتاج نص مشفر يتم تضمينه في معاملات التحويل المويجي ذات الترددات الواطئة – العالية (Low–High Coefficient) والحصول على صورة ذات نوعية جيدة وإمكانية استرجاع الرسالة المضمنة بشكل كامل وفك شفرتها وبدون الاعتماد على الصورة الأصلية (Blind Technique). أدت النتائج المطبقة على الصور الرقمية إلى الحصول على صور مضمنة للبيانات

(Stego image) ذات معامل ارتباط (Correlation Coefficient) عالي عند مقارنتها مع الصور الأصلية بالإضافة إلى أنها أعطت فروقات قليلة عند حساب القياسات (SNR, PSNR, MSE).
الكلمات المفتاحية: تشفير، إخفاء معلومات، تحويل مويجي، تقنية LSB.

1- المقدمة

ازداد استخدام إخفاء البيانات في السنوات الأخيرة نتيجة للتطور الحاصل في الإنترنت وتقنيات معالجة المعلومات، وكحلّ فعّال لحماية حقوق الطبع وسرية البيانات. إن إخفاء البيانات السرية (Secret data) في وسط غطاء (cover-media) سواء أكان (صورة أو إشارة، فيديو وملف نصي)، سيجعل المراقب على هذا الوسط أو المتطفل لا يعرف بوجود رسالة مخفية في هذا الوسط، إذ إن البيانات تضمن في الصورة (تكون محمولة في بيانات الصورة Embedding) وان معظم أنظمة الإخفاء تستخدم LSB والتي تستبدل مباشرةً البت الأخير من النقاط ((Least Significant Bit (LSB) في الصورة الغطاء (Cover Image) مع بت الرسالة السرية للحصول على الصورة السرية (Stego Image)[12] في بعض الأحيان قد يؤدي الإخفاء إلى تشويه الصورة الأصلية والتي هي صورة ليست قابلة لعدم فقدان البيانات بالإضافة إلى إن معظم طرق الإخفاء ليست جديرة بالقبول، كذلك بعض أنواع الصور (الصور العسكرية والطبية) غير مرغوب بها لفقدانها البيانات المضمنة فيها ولذلك تم استخدام الصور الرقمية، إذ إن نوعية(quality) الصورة المستعملة للإخفاء يجب أن تعطي صورة واضحة المعالم وفي نفس الوقت يجب إن تسترجع الصورة الأصلية بعد انتزاع الرسالة المضمنة والحصول على كامل الرسالة المضمنة أيضاً [6].

بعض الطرق تستخدم الحيز المكاني [3] وفيه يتم تضمين الرسالة السرية مباشرة إلى نقاط الصورة، ومن هذه الطرق (الأكثر شيوعاً) Histogram-Based و(LSB)، والتي تعطي أعلى قدرة (High-Capacity) واقل تشوه (Distortion) كخوارزميات Difference Expansion (DE). إذ اقترح Ni وآخرون [9] استخدام طريقة المدرج التكراري للإخفاء الذي استعمل الصفر والنقاط الضعيفة (Peak Point) للمدرج التكراري لصورة الغطاء لإخفاء الرسالة ولاستعادة الصورة الأصلية بعد انتزاع البيانات المضمنة.

إما الطرق الأخرى فتستخدم الحيز الترددي ومن أكثر الطرق حالياً والمستخدمة لإخفاء البيانات كالتحويل المويجي وتحويل Curvelet وDCT (Discrete Cosine Transform) والتي توفر قابلية عالية على المحافظة على حافات الصورة (عند الترددات العالية) وإمكانية تمثيل الصورة بتعدد القياس (Scale) والمكان (Location) .

2- الإعمال السابقة:

يعد موضوع إخفاء المعلومات وتشفيرها من المواضيع التي تم العمل بها مبكراً وطورت بشكل سريع ومتقدم مع دخول عالم الصور الرقمية والتي كانت محط اهتمام العديد من الباحثين في أدناه عدداً من الدراسات في هذا المجال:

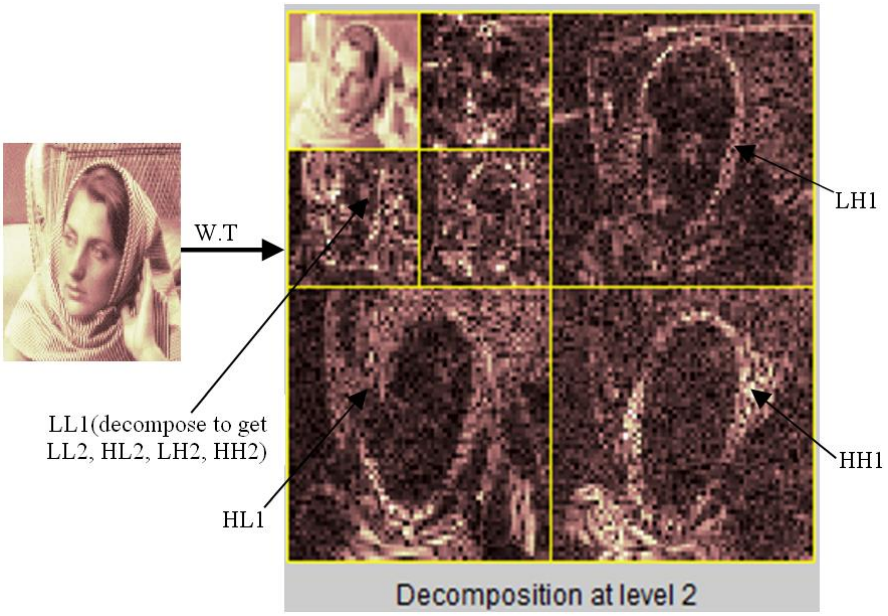
- اقترح الباحث Eman (2008) طريقة لإخفاء البيانات في الصور الثنائية، إذ يتم أولا تحديد النقاط الضوئية التي يمكن أن تنقلب دون حدوث تشوهات مرئية في الصورة المضمنة وذلك عن طريق استخدام مجموعة من القوانين التي يتم من خلالها فحص جميع النقاط المجاورة لنقطة المركز لكل قطاع غير منتظم ومن ثم يتم تغيير النقطة المركزية فقط في حالة مطابقة القطاع لهذه الشروط وهذه الخاصية تسمح باكتشاف البيانات المضمنة دون الرجوع إلى الصورة الأصلية، وقد أظهرت التجارب نتائج مختلفة لصور ثنائية مختلفة.

- وقدم الباحث A.A. Abdul Latef (2011) طريقة للإخفاء في الصور الملونة عن طريق تقسيمها إلى أربع أجزاء متساوية كل جزء متكون من ثلاثة قنوات (Red, Green, Blue) يتم اختيار احد هذه القنوات لكل جزء بالاعتماد على نسبة اللون العالية في ذلك الجزء، بعدها يتم تطبيق التحويل المويجي على الجزء المختار، كما يتم تقسيم الرسالة المراد إخفائها إلى أربع أجزء أيضاً وتطبيق DCT عليها بعدها تضمن كل جزء منها في الترددات العالية للتحويل المويجي لأحد أجزاء صور الغطاء للحصول على الصورة السرية.
- أما الباحث Yong (2011) اقترح مخطط لإخفاء البيانات السرية داخل الصورة باستعمال تحويل curvelet إذ يتم تشفير الصورة المراد إخفائها باستخدام تحويل (Radon) واستخدام معاملات الترددات العالية للتحويل curvelet لتضمين البيانات.
- قام الباحث Chin (2005) باقتراح طريقة لإخفاء صورة بتغيير معاملات التحويل لصورة الغطاء (مثلاً DCT)، إذ يتم إبدال كل بت من الصورة المراد تضمينها ببت من احد معاملات التحويل، إذ تبين أن التحويل المستخدم يوفر نسبة ضغط عالية للصورة المضمنة والمحافظة على نوعية الصورة، كما تم استخدم خوارزمية التشفير DES للبيانات المراد تضمينها قبل عملية التضمين لتوفير سرية.
- اقترح الباحثان Maity وKundu (2004) تقنيات العمياء لإخفاء العلامة المائية (watermarking blind) عن طريق تضمين العلامة المائية في المعاملات الترددية الواطئة للتحويل المويجي متعدد المستويات للصور الملونة (multilevel wavelet LL)، إذ تم تضمين العلامة في حزمة اللون الأحمر (Red band) للمعاملات الترددية الواطئة.
- اقترح الباحثان Abdelwahab و Hassan (2008) استعمل المستوى الأول من التحويلات المويجية في إخفاء البيانات وتضمينها ولكن كانت البيانات المنتزعة ليست مماثلة كليا إلى النسخة المضمّنة.

3- التحويلات المويجية ثنائية الإبعاد:

إن التحويلات المويجية ثنائية الإبعاد هي تحويلات ثنائية الإبعاد تعمل على تمثيل الصورة بعدة مواقع (Location) وبتعدد القياس (Scale) تعمل على تجزئة الصورة ثنائية الإبعاد إلى حزم ترددية واطئة الترددLow-Low) تسمى (الصور الناعمة smooth image) وإلى حزم ترددية عالية التردد (Low-High, High-Low, High-High) تسمى (الصور التفصيلية detailed image). أي تعمل على تقسيم الصورة إلى أربع صور LL1, LH1, HL1, HH1 والتي تمثل المستوى الأول، وللحصول على المستوى الثاني سيتم استخدام الصورة LL1 للحصول على أربع صور أخرى هي LL2, LH2, HL2, HH2 وهكذا لبقية المستويات وكما في الشكل (1).[7]

التحويل المويجي يقدّم مهام واسعة في معالجة الصورة، إذ أن معاملاته تعطي درجة عالية من الترابط والتناسق مع مميزات النظام البصري الإنساني، فعند دراسة النظام البصري يتبين أن أي تعديل طفيف على الترددات العالية من الصعب رويته بالعين البشرية [11]. لذلك سنستخدم في هذا البحث الترددات الواطئة – العالية (LH) في تضمين الرسالة السرية.



الشكل (1). التحويل الموجي لصورة Barbara لمستويين

4- التشفير بطريقة Keyword Mixed Transposition

تم اعتماد الطرق التعويضية كإحدى الطرق المعتمدة لتشفير النصوص والتي تعمل على إبدال النص بنص أخر ومنها طريقة خلط الأبجدية (mixed alphabet) التي تولد خليط من الحروف الأبجدية بالاعتماد على مفتاح أبجدي (alphabet)عشوائي يتم اختياره لغرض تشفير الرسالة إذ تشفر النص (المسمى plain text) باعتماد مفتاح أبجدي عشوائي لتوليد خليط من الأحرف الأبجدية (النص المشفر cipher text)، كما في الخطوات التالية:

1- إدخال المفتاح والذي هو عبارة عن كلمة عشوائية بدون تكرار للحروف (مثلا إدخال كلمة william ستصبح wilam) تتراوح بين 1-26 حرف أي ما يعادل (!26 تقريباً 1 بليون حرف مما يجعلها من الطرق الجيدة في التشفير). إذ يتم كتابة الكلمة في سطر والسطور التي بعده سوف تمثل جميع الحروف الأبجدية التي لم تظهر بالكلمة وكما يلي:

w	i	l	a	m
b	c	d	e	F
g	h	j	k	N
o	p	q	r	S
t	u	v	x	Y
z				

2- بعدها تؤخذ الحروف من المصفوفة العلوية عمود عمود ونضعها تحت الحروف الأبجدية وكما يلي:

alphabit	a	b	c	d	e	f	j	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	Y	z
cipher	w	b	g	o	t	z	i	c	h	p	u	l	d	J	q	v	a	e	k	r	x	m	F	n	s	y

3- بعد أن حصلنا على الـ cipher يتم إدخال النص المراد تشفيره plain text (مثلا help) كل حرف من النص يؤخذ ما يقابل alphabet من حرف cipher لتعطي الرسالة المشفرة (ctlv).

4- ولاسترجاع النص الأصلي من النص المشفر يتم اعتماد ذات الطريقة مع اخذ قيم alphabet بدل من الـ cipher (التي تمثل النص المشفر).

إن هذه الطريقة لا تتعامل فقط مع الحروف الأبجدية بل مع الأرقام مثلاً إذ يتم تعويضها بذات القيمة (مثلا الرقم 1 سيعوض عنها بالرقم 1 في النص المشفر بدون تغيير)[10].

5- الطريقة المقترحة لإخفاء البيانات واسترجاعها:

لغرض إخفاء البيانات سنفترض إن C عبارة عن صورة ملونة التي تمثل صورة الغطاء بإبعاد $M_c \times N_c$ والتي تمثل بالمعادلة (1):

$$C=\{x_{ij} \mid 0\le i<M_c,\ 0\le j<N_c,\ x_{ij}\in\{0,1,\ \ldots\ldots,\ 255\}\} \quad \ldots(1)$$

و M تمثل n-bit الرسالة السرية وتمثل بالمعادلة (2):

$$M=\{m_i \mid 0\le i<n,\ m_i\in\{0,1\}\} \quad \ldots(2)$$

ولنفترض أن n-bit للرسالة السرية سوف يتم تضمينها في k-rightmost LSB للصورة الغطاء C.

سوف نتبع خطوات الخوارزمية التالية لإخفاء البيانات (انظر الشكل 2):

1- التقاط الصورة C.

2- تعيير الصورة لتصبح ضمن الإبعاد القياسية التي تم اعتمادها خلال البحث إذ يتم معالجة الصورة بإبعاد [512, 512].

3- تحويل الصورة إلى صورة رمادية (gray scale).

4- حساب معاملات التحويل المويجي للصورة C إذ تم اعتماد المستوى الأول أو المستوى الثاني.

5- حساب حد العتبة للمعاملات Low-high.

6- حساب عدد المواقع التي يمكن تضمين الرسالة بها لتحديد أعلى حد لعدد البت التي يمكن تضمينها.

7- إدخال البيانات الرسالة السرية M وقراءتها من ملف نصي (Text file) ومفتاح (k عبارة عن كلمة) إذ يتم تشفر النص بطريقة Keyword mixed transposition باعتماد المفتاح k والحصول على نص مشفر يتم تحويله من الشكل الرقمي (Decimal) إلى الشكل الثنائي (Binary).

8- يتم إضافة حجم الرسالة إلى السطر الأول (Row) لغرض استرجاع الرسالة.

9- لكل قيمة ضمن ((Low-high(LH(i,j) يتم مقارنتها مع حد العتبة إذا كانت اقل منه يتم تحويلها إلى الشكل الثنائي وإبدال البت LSB بالبت من M_i للحصول على cover image، إذ أن i,j تمثل مؤشرات إلى احد المعاملات للصور الرقمية.

10- إرجاع قيمة ((Low-high(LH(i,j إلى الشكل الرقمي وتكرارها إلى أن يتم إضافة جميع قيم الرسالة.

11- بعد إضافة الرسالة يتم أعادة تركيب المعاملات للتحويل المويجي للحصول على الصورة المتضمنة للرسالة (stego image).

ولاستعادة النص والحصول على الرسالة المشفرة نتبع الخطوات التالية كما في الشكل (3):

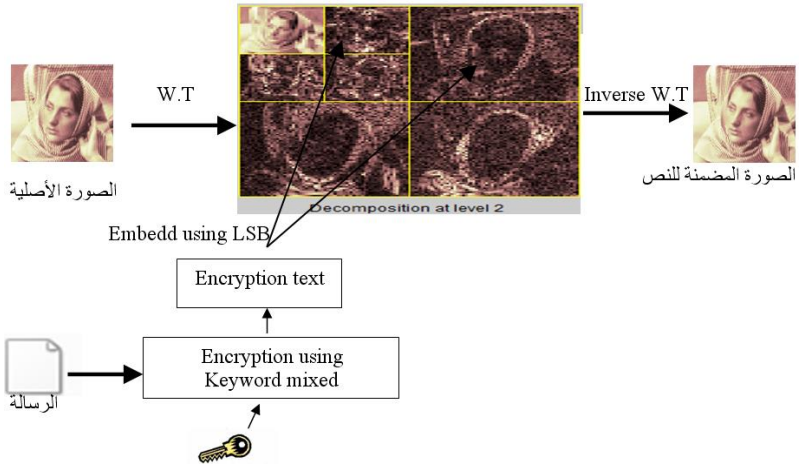
1- حساب معاملات التحويل المويجي للصورة stego image التي تم الحصول عليها بعد استقبالها أو التي تم الحصول عليها من الوسط media والتي تحتوي على النص المشفر إذ تم اعتماد المستوى الأول أو المستوى الثاني وإدخال المفتاح (k).

2- حساب حد العتبة للمعاملات Low-high .

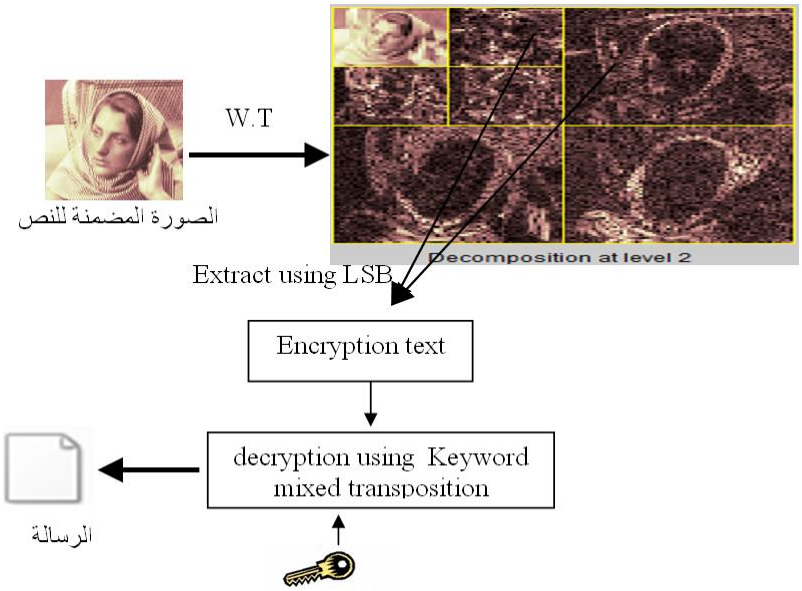
3- الحصول على حجم الرسالة من السطر الأول (Row) للمعاملات Low-high لغرض استرجاع الرسالة.

4- لكل قيمة ضمن Low-high(LH(i,j)) يتم مقارنتها مع حد العتبة إذا كانت اقل منه يتم تحويلها إلى الشكل الثنائي واخذ البت LSB ووضعه في Mi تكرر العملية إلى أن يتم الوصول الحصول على جميع البت المضمنة.

5- تحويل الـ Mi إلى الشكل الحرفي (character) وإدخاله مع المفتاح إلى طريقة Keyword mixed transposition لفك شفرة النص والحصول على الرسالة السرية.



الشكل (2). الطريقة المقترحة لإخفاء نص داخل معاملات التحويل المويجي



الشكل (3). الطريقة المقترحة لاسترجاع نص من داخل معاملات التحويل المويجي

6- النتائج:

لغرض التجربة تم اختيار عدد من الصور الرقمية (ذات الامتداد tiff, bmp, png و jpg) ذات الحجم [512, 512] لصورة الغطاء (cover image) والتي يمكن ملاحظتها بالشكل ((4) للصور a,b,c) إذ تم اعتماد النص التالي (338 حرف ما يعادل 2704 بت):

A digital image processor is the heart of any image processing system. An image processor consists of a set of hardware modules that perform four basic functions: image acquisition, storage, low-level (fast) processing, and display. Typically, the image acquisition module has a TV signal as the input and converts this signal into digital form, both spatially and in amplitude.

واعتماد المفتاح (findyou) لاستخدامه في تشفير وفك تشفير النص السابق وإعطاء النص التالي:

Alhihefx hnfir pzjgrddjz hd ebr brfze jw fco hnfir pzjgrddhci dodern. Ac hnfir pzjgrddjz gjcdhded jw f dre jw bfzlvfzr njlkxrd ebfe przwjzn wjkz afdhg wkcgehjcd: hnfir fgtkhdhehjc, dejzfir, xjv-xrqrx (wfde) pzjgrddhci, fcl lhdpxfo. Tophgfxxo, ebr hnfir fgtkhdhehjc njlkxr bfd f TV dhicfx fd ebr hcpke fcl gjcqrzed ebhd dhicfx hcej lhihefx wjzn, ajeb dpfehfxxo fcl hc fnpxheklr.

يتم تحويل هذا النص إلى الشكل الثنائي وتضمينه داخل معاملات التحويل المويجي حسب الطريقة المقترحة في الفقرة 5 لتكوين صورة مضمنه للنص (stego image) كما في الشكل ((4) للصور d,e,f) التي من الممكن إرسالها إلى المستلم وعند استلامها من الطرف الأخر (المستلم Reciver) يتم استرجاع النص المشفر باعتماد الطريقة المقترحة المذكورة أنفا ولفك تشفير النص المسترجع من الصورة المضمنة له ويجب استخدام نفس المفتاح (findyou) للحصول على الرسالة التالية:

Adigital image processor is the heart of any image processing system. An image processor consists of a set of hardware modules that perform four basic functions: image acquisition, storage, low-level (fast) processing, and display. Typically, the image acquisition module has a TV signal as the input and converts this signal into digital form, both spatially and in amplitude.

من خلال الجدول (1) والشكل (5) نلاحظ أن معامل الارتباط متقارب جداً (بين الصورة الأصلية والصورة المضمنة للرسالة Stego image)، كذلك يمكن ملاحظة الفرق الطفيف بين هذه الصور من خلال المقاييس (MSE, PSNR, SNR) والتي يتبين بشكل واضح أن تتأرجح حول محور مستقر تقريباً، كذلك يلاحظ من الجدول (1) الذي يقدم استقرارية الخوارزمية والتصرف الطبيعي للخوارزمية والتي تم تطبيقها عملياً، إذ تبين إن معاملات الترددات الواطئة–العالية للتحويل المويجي جيدة جداً لإخفاء البيانات من دون إن توثر على نوعية وجودة الصورة ودون أن تحس العين البشرية بأي تغيير طفيف على الصورة الناتجة وان اقتراب الصورة الأصلية مع الصورة المضمنة للنص السري كان جيد مما يدعم كون الخوارزمية المعتمدة جيدة للإخفاء.

الجدول (1). قيم المعاملات (SNR, PSNR, MSE) ومعامل الارتباط

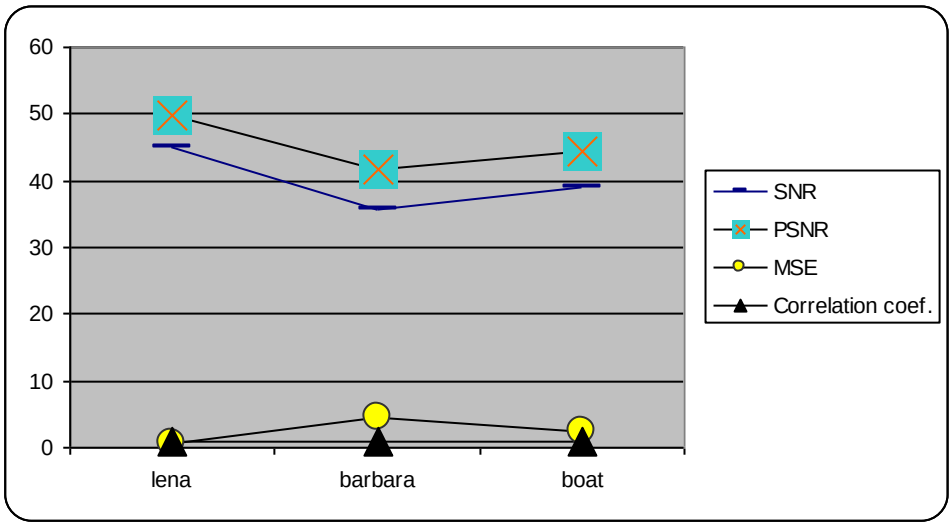
Image	SNR	PSNR	MSE	Correlation coefficient
lena	44.09	49.75	0.68	0.9998
barbara	35.84	41.73	4.36	0.9993
boat	39.13	44.48	2.31	0.9995

a *b*

c *d*

e *f*

الشكل (4). يمثل بعض الصور الأصلية (a, b, c) والصور المضمنة للنص (stego image) بعد تضمين النص باعتماد الطريقة المقترحة بالبحث



الشكل (5). رسم بياني للمعاملات (MSE, PSNR, SNR ومعامل الارتباط)

7- الاستنتاجات:

إن اعتماد معاملات الترددات الواطئة– العالية للتحويل المويجي للصور الرقمية وطريقة LSB لإخفاء البيانات توفر استقرارية عالية والتي اعتمدت من قبل الكثير من الباحثين مع الصور الطبيعية والجوية. وعند استخدام خوارزمية التشفير keyword mixed transposed يتم توليد خليط من الأحرف الأبجدية التي تكون من الصعب فك تشفيرها لأنه لغرض فك شفرتها يحتاج الشخص المتطفل إلى (!26) ووقت طويل جداً لفك شفرتها. إن اعتماد الخوارزمية المقترحة في البحث أعطت إمكانية عالية في تشفير وإخفاء البيانات ومقدار عالي من الارتباط بين الصورة الأصلية والمضمنة للنص وأعلى مقاييس(PSNR, MSE, SNR) وهذا ما تم ملاحظته في الجدول (1) والشكل (5).

8- الإعمال المستقبلية:

إمكانية اعتماد الشبكات العصبية كمعيار لقياس مدى التقارب بين الصورة الأصلية والصورة المضمنة للنص المشفر، وإمكانية اعتماد المعاملات العالية –الواطئة والعالية – العالية للتحويل المويجي لإخفاء البيانات واستخدام خوارزميات تشفير أقوى وأفضل كخوارزميات DES و RSA التي تعمل على توليد أكثر من مفتاح احدها عام والآخر خاص، وإمكانية الاعتماد أكثر من بت لإخفاء البيانات.

المصادر

[1] A.A. Abdul Latef, (2011), "Color Image Steganography Based on Discrete Wavelet and Discrete Cosine Transforms", IBN AL- HAITHAM J. FOR PURE & APPL. SCI. VOL.24 (3).

[2] A.A. Abdelwahab, L.A. Hassan, (2008), "A discrete wavelet transform based technique for image data hiding", in: Proceedings of 25th National Radio Science Conference, Egypt.

[3] Celik, M., G. Sharma, A. M. Tekalp, and E. Saber,(2002), "Reversible data hiding", Proceedings of the International Conference on Image Processing, Rochester, NY, September.

[4] Chin-Chen Chang, (2005), "A DCT-domain System for Hiding Fractal Compressed Images", Proceedings of the 19th International Conference on Advanced Information Networking and Applications (AINA'05),Vol.2.

[5] Eman Th. Sedeek Al-obaidy,(2008), "An Algorithm for Data Hiding in Binary Images", Raf. J. of Comp. & Math's., Vol. 5, No. 2, 8.

[6] Huang, Hui-Yu. and Shih-Hsu Chang, (2011), "Lossless Data-hiding Technique based on Wavelet Transform", MVA2011 IAPR Conference on Machine Vision Applications, June 13-15.

[7] I. Daubechies, (1992), "Ten lectures on wavelets", Philadelphis, PA: SIAM.

[8] Maity S.P. and Kundu M.K., (2004), "A Blind CDMA Image Watermarking Scheme in Wavelet Domain", IEEE International Conference:2633 – 2336.

[9] Ni, Z., Y.Q. Shi, N. Ansari, and W. Su, (2003), "Reversible data hiding", in Proc. of 2003 Int. Symposium on Circuits and Systems, pp. II-912-915.

[10] William stallings, (1999), "Cryptography and network security: principle and practice 2nd ed", Prentice hall. upper saddle river, New Jersey 07458.

[11] Xuan G., C. Yang, Y. Zheng, Y.Q. Shi and Z. Ni, (2004), "Reversible data hiding based on wavelet spread spectrum", IEEE International workshop on multimedia signal processing (MMSP2004), Siena, Italy.

[12] Yang H., Xingming Sun and Guang Sun, (2009), "A High-Capacity Image Data Hiding Scheme Using Adaptive LSB Substitution", Radioengineering, Vol. 18, No. 4.

[13] Yong Hong Zhang, (2011), "Digital Image hiding using curvelet transform", IEEE Conference.