International Science and Technology Journal
المجلة الدولية للعلوم والتقنية
Volume 36 العدد
Part 2 المجلد
المجلة الدولية للعلوم والتقنية
International Science and Technology Journal
ISTJ

http://www.doi.org/10.62341/amsz1803

Received	2025/03/10	تم استلام الورقة العلمية في
Accepted	2025/04/09	تم قبول الورقة العلمية في
Published	2025/04/11	تم نشر الورقة العلمية في

زيادة سعة إخفاء البيانات في الصورة الرقمية الرمادية باستخدام خوارزمية خانة الإشارة المعدلة MSD

أ.ام السعد محمد الاميلس

قسم الهندسة الالكترونية – كلية التقنية الصناعية – مصراته - ليبيا
om.2017.cit@gmail.com

الملخص

في هذه الورقة تم اجراء تحليل ودراسة تجريبية لخوارزمية خانة الإشارة المعدلة (MSD) Modified Signed–Digitوهي طريقة تهدف الي إخفاء كمية من البيانات السرية والمتمثلة في صورة رمادية بحجم 512 × 512 في مجموعة من صور الغلاف وقد تم مناقشة بعض مقاييس الجودة مثل نسبة الإشارة إلى الضوضاء (PSNR) ومتوسط مربع الخطأ (MSE) وسعة التضمين (BPP)، وكذلك حساب عدد صور الغلاف الأمثل بالإضافة الي حساب الزمن المستغرق في عملية الاخفاء والذاكرة المستهلكة. تم اجراء التجارب على أربع صور سرية بدرجات الرمادي، ولحجمين مختلفين من صور الغلاف، حيث يتم تحديد عدد صور الغلاف المطلوبة للصورة السرية وفقًا لبعض المدخلات مثل عدد البكسلات n في كل مجموعة من صورة الغلاف وعدد البتات في كل كتلة من الصورة السرية L=n+1 . كما أجريت التجارب باستخدام برنامج الماتلاب وبأربع قيم مختلفة لـ n،(2,3,4,5) وقد حاولنا إيجاد أفضل قيمة لعدد البتات في كل كتلة L من الصورة السرية وفي كل حالة من n لتحقيق أفضل حالة لجودة الصورة PSNR، MSE بالنسبة لكلا حجمي صورة الغلاف، ومن ناحية أخرى، استهلاك ذاكرة وقت أقل.

بمقارنة النتائج عند أحجام مختلفة من صور الغلاف، وجد أنه كلما تم استخدام حجم أكبر، فإننا نحتاج إلى عدد أقل من صور الغلاف، واستهلاكًا أقل للوقت. من ناحية أخرى، نحتاج إلى المزيد من استهلاك الذاكرة. بالنسبة للمقاييس الأخرى، PSNR وMSE وسعة التضمين BPP، فقد تم الحصول على نتائج متقاربة.

http://www.doi.org/10.62341/amsz1803

وأخيرا يظل الاختيار الأفضل مرتبطا بالمستخدم ونوع التطبيق او الأداء المطلوب هل في جودة الصورة أم في أقل استهلاك للذاكرة والوقت مع سعة تضمين أكبر.

الكلمات المفتاحية: خوارزمية MSD، نسبة الإشارة إلى الضوضاء (PSNR)، خطأ التربيع المتوسط (MSE)، سعة التضمين، بت لكل بكسل(BPP)، استهلاك الذاكرة، استهلاك الوقت.

Increasing data hiding capacity in grayscale digital image using modified signal digit algorithm

Om Essad Mohamed Lamiles
Department of Electronic Engineering - College of Industrial Technology – Misurata - Libya
om.2017.cit@gmail.com

ABSTRACT

In this paper, an experimental analysis and study of the Modified Signed-Digit (MSD) method was conducted, which aims to hide a quantity of secret data represented in a grayscale image of size 512 × 512 in a set of cover images. Some quality metrics such as signal-to-noise ratio (PSNR), mean squared error (MSE), and embedding capacity (BPP) were measured. As well as calculating, the optimal number of cover images, the time taken in the hiding process, and the consumed memory. The experiments were conducted two different sizes of cover images, where the number of cover images required for the secret image is determined according to some inputs such as the number of pixels n in each group of the cover image and the number of bits in each block of the secret image L=n+1. Also, four different values of n, (2, 3, 4, 5). We tried to find the best value for the number of bits in each block L of the secret image and in each case of n to achieve the best case for image quality PSNR, MSE for both cover image sizes, and on the other hand, less time memory consumption.

By using the Matlab program, we compared the results at different cover image sizes, we found that as the larger size used, the fewer cover images are needed and less time consumption. On the other hand, more memory consumption. For the other metrics, PSNR, MSE and BPP, close results were obtained.

Finally, the best choice remains related to the user and the type of application or the required performance, whether in image quality

http://www.doi.org/10.62341/amsz1803

or in less memory and time consumption with a larger embedding capacity.
Keywords: MSD algorithm, Signal-to-noise ratio (PSNR), Mean square error (MSE), Bit-per-pixel (BPP), Memory consumption, Time consumption.

1. المقدمة

عملية إخفاء المعلومات (Steganography) هي تقنية تُستخدم لحماية الرسائل من الوصول غير المصرح به، ويمكن ترجمتها إلى "الكتابة المغطاة". يعود أصل الكلمة إلى اللغة اليونانية، حيث تعني كلمة "ستيغانو" (Stegano) "مغطى"، بينما تعني كلمة "جرافي" (Graphy) "كتابة". تعتمد هذه التقنية على تضمين البيانات في وسائط أخرى، مثل النصوص والصور ومقاطع الفيديو والصوت، بطريقة تجعل البيانات غير مرئية أو واضحة للمستخدمين العاديين[1] .

الهدف الأساسي في أي عملية إخفاء Steganography هو إخفاء أكبر قدر من البيانات السرية مع الحفاظ على جودة الغطاء سواء كان صورة او فيديو او صوت، وكذلك ضمان سلامة البيانات السرية.

تم في هذه الورقة استخدام الخوارزمية MSD لتقليل عدد التعديلات المطلوبة وذلك بتوزيع البيانات بشكل ذكي على بكسلات الصورة الرمادية باستخدام عمليات المودولو (modulo)والذي يضمن توزيع البيانات المخفية بطريقة يصعب اكتشافها مع الحفاظ على جودة الصورة. ومن ثم قياس أداء هذه الطريقة باستخدام مجموعة من مقاييس الأداء ومن ضمن هذه المقاييس مقياس نسبة الإشارة الى الضوضاء PSNR، مقياس مربع الخطأ MSE، ومقياس معدل الخطأ في البتات BER وكذلك قياس مدي استهلاك الوقت والذاكرة memory and time consumption.

2. تاريخ إخفاء البيانات

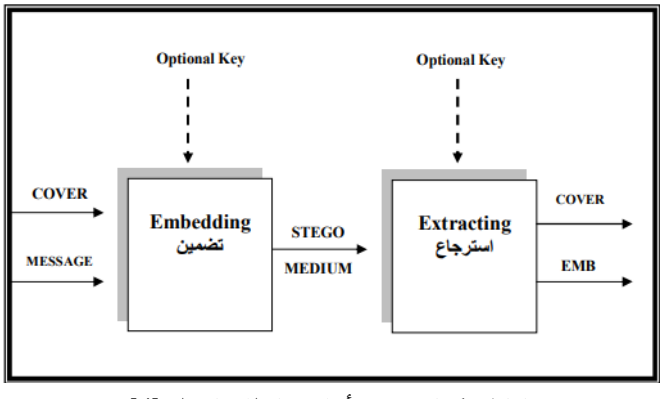
إخفاء البيانات علم قديم يعود إلى آلاف السنين، وكان يستخدم في الثقافات القديمة لتبادل الرسائل السرية بدأ استخدام تقنيات إخفاء الرسائل في الحضارة اليونانية، حيث يُقال إن الإغريق استخدموا طرقًا مثل "الشمع المزدوج"، إذ كانوا يكتبون الرسائل على ألواح خشبية ثم يغطونها بطبقة من الشمع لتبدو كألواح فارغة[1].

في القرن الخامس قبل الميلاد، استخدم "هيرودوت"، المؤرخ اليوناني، بعضًا من أقدم أساليب إخفاء البيانات التي تم توثيقها، حيث روى قصة عن كيفية إخفاء رسالة عبر نقشها على رأس أحد عُماله، ثم تغطيتها بالشعر لإخفاء محتوى الرسالة عن الأعداء.

http://www.doi.org/10.62341/amsz1803

مع مرور الوقت، تطورت التقنيات المستخدمة في إخفاء المعلومات. على سبيل المثال، في الحربين العالميتين الأولى والثانية، استخدمت الدول المتحاربة تقنيات جديدة لإخفاء الرسائل داخل الصور أو من خلال إشارات معينة، وذلك لتجنب اكتشاف الاتصالات السرية[2][3] .

في العصر الرقمي، بدأ إخفاء البيانات يأخذ طابعًا تقنيًا، حيث أصبح يستخدم في حماية المعلومات الرقمية داخل وسائط مثل الصور والفيديوهات والملفات الصوتية. تطورت أساليب الإخفاء باستخدام تقنيات الحوسبة، حيث بدأ لاعتماد على طرق مثل تعديل البتات الأقل أهمية (LSB) والبتات ذات الأهمية العليا(MSB) ، لتخزين البيانات السرية داخل ملفات الوسائط دون التأثير الملحوظ على جودة الوسائط .[4][5]الشكل (1) يوضح النموذج الأساسي لنظام التغطية.



الشكل.1 النموذج الأساسي لنظام التغطية[4]

3. الدراسات السابقة

إحدى أكثر التقنيات شيوعًا هي طريقة الاخفاء في البت الأقل اهمية LSB، حيث إنها بسيطة وسريعة وتتمتع بجودة صورة مضمنة جيدة. في هذه الطريقة، يتم تقسيم الصورة السرية الثنائية إلى كتل تحتوي على L بت، ثم تضمين كل كتلة L في البت الأقل اهمية LSB لكل بكسل من صورة الغلاف، حيث n ≤8 أو L ≤1. بشكل عام، يمكن لهذه الطريقة تحقيق جودة صورة جيدة عندما 3 ≤ L عدد البتات المخفاة في بكسل صور الغلاف، ولكن عندما. 4 ≤L، فان جودة الصورة تنخفض بشكل كبير [5].

لتحسين طريقة الاخفاء في البت الأقل اهمية LSB، تم اقتراح العديد من طرق الاخفاء، ففي عام 2001، اقترح Wang, & Lin طريقة تستخدم LSB الأمثل والخوارزمية الجينية،

http://www.doi.org/10.62341/amsz1803

حيث يتم تقديم الخوارزمية الجينية لحل مشكلة إخفاء البيانات في LSBs لصورة الغلاف عندما تكون L كبيرة من أجل تحسين جودة الصورة وسعة التضمين[6].

في عام 2006 اقترح Jarno, M تعديلاً على طريقة LSB يستخدم زوجًا من البكسلات من صورة الغلاف كمجموعة، حيث يتم نقل البتات السرية في LSB'sمن بكسلين. لذلك فإن هذه الطريقة لها نفس الحمولة مثل طريقة استبدال LSB، ولكن مع تغييرات أقل على بكسلات صورة الغلاف. لذا فإن أداء هذه الطريقة أفضل من طريقة LSB، ويتم استغلال اتجاه التعديل على بكسلات الغلاف لإخفاء البيانات، ولكن يوجد اتجاهان مختلفان للتعديل يتوافقان مع نفس زوج البتات السرية المراد تضمينها، مما يعني أن الاستغلال غير مكتمل .[7]

كما اقترح Zhang وWang في عام 2006 طريقة جديدة تسمى استغلال اتجاه التعديل (EMD). الفكرة الرئيسية لطريقة EMD هي استخدام مجموعة منفصلة من n بكسل من صورة الغلاف لتضمين الرقم التالي من (2n+1)−ary k−digit التي تمثل كتلة البت L التالية من إدخال الصورة السرية ويمكن تغيير بكسل واحد فقط في المجموعة بمقدار ±1. لذلك، تتمتع هذه الطريقة بجودة صورة جيدة جدًا وقدرة تضمين أفضل، ولكن تقل قدرة التضمين مع زيادة n [8].

لتحسين طريقة EMD اقترح Lee واخرون طريقة EMD المحسنة (IEMD) في عام 2007حيث تستخدم هذه الطريقة بكسلين من صورة الغلاف للمجموعة و8−ary كدالة استخراج. تتمتع هذه الطريقة بسعة تضمين أكبر من EMD، لكنها تستخدم بكسلين فقط في المجموعة ولا يمكنها استخدام المزيد[9].

في عام 2013 قدم Kuo and Wang طريقة GEMD [10]، حيث تستخدم n بكسل من صورة الغلاف لتضمين n + 1 بت، ويمكن تغيير قيمة بكسل واحدة على الأقل في كل مجموعة بمقدار ±1. أيضًا في هذه الطريقة لا توجد حاجة للتحويل، حيث حافظت GEMD على جودة صورة جيدة وقدرة تضمين جيدة، ويمكنها أيضًا ضبط حجم البكسل .n

في عام 2015، قدم الباحثان Kuo & Wang دراسة بعنوان "Signed digit data hiding scheme"، حيث اقترحا تقنية جديدة لإخفاء البيانات تعتمد على خوارزمية MSDأظهرت النتائج أن هذه التقنية توفر سعة إخفاء أكبر مع تقليل التشوه في الصور المضمنة[11].

http://www.doi.org/10.62341/amsz1803

في عام 2016، نشر الباحثون Chang, Hu & Lin دراسة بعنوان "Reversible Shared Data Hiding Based on Modified Signed Digit EMD". اقترحت الدراسة خوارزمية جديدة لإخفاء البيانات القابلة للعكس تعتمد على MSD وEMD، مما يسمح باستعادة الصورة الأصلية بالكامل بعد استخراج البيانات المخفية [12] .

في عام 2020، قدم الباحث Solak دراسة بعنوان "High Embedding Capacity Data Hiding Technique Based on EMSD and LSB Substitution Algorithms". اقترحت الدراسة تقنية هجينة لإخفاء البيانات تعتمد على خوارزمية MSDالمحسنة (EMSD) واستبدال البت الأقل أهمية(LSB) ، مما أدى إلى زيادة سعة الإخفاء مع الحفاظ على جودة الصورة[13] .

4.مقاييس الأداء

يعتبر استخدام مقاييس الأداء في تطبيقات تحسين الصور الرقمية له أهمية كبيرة في معرفة كفاءة التحسين الحاصلة لها، وواحدة من أهم العمليات على الصورة، من ضمن هذه المقاييس:

1.4 مقياس نسبة الإشارة إلى الضوضاء Peak Signal to Noise Ratio

يتم تطبيق هذا المصطلح على الصور كمقياس للجودة، وهو يشير إلى نسبة الإشارة إلى الضوضاء حيث يعبر عن النسبة بين القيمة القصوى الممكنة للإشارة وقوة الوضاء المشوهة التي تؤثر على جودة تمثيلها كما في المعادلة التالية[14]:

$$PSNR = 10\ log_{10}\left[\frac{R^2}{MSE}\right] \qquad (1)$$

حيث:

R^2: هي القيمة القصوى للإشارة الموجودة في الصورة الأصلية.

MSE: هو متوسط الخطأ التربيعي بين الصورة الأصلية أو صورة الغطاء cover image وبين الصورة الناتجة بعد عملية الإخفاء stego image. [14]

2.4 مقياس مربع الخطأ Mean Squared Error

يتم قياس مربع الخطأ MSE للصورة الرمادية حسب المعادلة التالية[14] :

$$\mathrm{MSE} = \frac{1}{\mathrm{MN}} \sum_{0}^{\mathrm{m}-1} \sum_{0}^{\mathrm{n}-1} [\mathrm{I}_1(\mathrm{i},\mathrm{j}) - \mathrm{I}_2(\mathrm{i},\mathrm{j})]^2 \qquad (2)$$

http://www.doi.org/10.62341/amsz1803

حيث:

M,N : عدد الصفوف و الأعمدة للصورة الغطاء و الصورة الناتجة.

$I_1(i,j)$: قيمة البكسل في الصورة الغطاء cover image قبل الإخفاء عند النقطة (i,j).

$I_2(i,j)$: قيمة البكسل في الصورة الناتجة stego image عند النقطة (i,j) .

3.4 مقياس عدد البتات لكل بكسل Bit Per Pixel

يتم تعريف البتات لكل بكسل (BPP) على أنها القيمة المتوسطة للتضمين لكل بكسل في الصورة، بغض النظر عن حجم الصورة. ويمكن حسابها عن طريق قسمة حجم التضمين الإجمالي على عدد البكسلات في الصورة. ويتم حسابه حسب المعادلة التالية[11]:

$$\mathrm{bpp}_{\mathrm{MSD}} = \frac{\log_2(\mathrm{tn})}{\mathrm{n}} \qquad (3)$$

حيث:

n : عدد البتات المطلوبة لكل كتلة من صور الغطاء.

t_n : الـ Modulo المستخدم ويتم حسابه حسب الصيغة التالية[11]:

$$t_n = \begin{cases} 2 \times \left(\frac{4^{\lfloor \frac{n+1}{2} \rfloor}-1}{3}\right)+1, & n \ \ is \ \ odd, \\ 4 \times \left(\frac{4^{\lfloor \frac{n}{2} \rfloor}-1}{3}\right)+1, & n \ \ is \ \ even. \end{cases} \qquad (4)$$

5. خوارزمية خانة الإشارة المعدلة MSD: –

في هذه الورقة تم العمل على طريقة MSDباستخدام الصور الرمادية وهي تقنية تُستخدم لتمثيل الأرقام الثنائية بطريقة خاصة تتيح استخدام إشارات موجبة وسالبة لتقليل الحمل الحسابي، وبالتالي تحسين الأداء والمرونة في العمليات الحسابية لإخفاء صورة رمادية سرية داخل صورة رمادية أخرى حيث سيتم إخفاء بتات الصورة السرية في كل بكسل من بكسلات الصورة الغطاء بناءً على شروط معينة.

تستخدم خوارزميةMSD تقنية تعتمد على الوزن والمودولو (Modulo)في تعديل قيم البكسلات. تعتمد هذه الطريقة على توزيع البيانات السرية على أكثر من بيكسل في

http://www.doi.org/10.62341/amsz1803

الصورة. حيث يتم تقسيم البكسلات إلى مجموعات، ويُطبق على كل مجموعة عملية الـ modulo، وتُستخدم النتيجة لتحديد قيمة التعديل للبيكسل[11].

بعد تعديل البكسلات، يتم التحقق من جودة الصورة للتأكد من أن التعديلات لم تسبب أي تشوه بصري واضح. غالبًا ما تكون التعديلات طفيفة جدًا بحيث لا يمكن ملاحظتها بالعين المجردة. لاسترجاع النص أولاً، يقوم المستقبل بتحليل الصورة باستخدام نفس طريقة توزيع الأوزان التي تم استخدامها في الإخفاء. ويتم تطبيق العملية العكسية لعملية الـ Modulo على البكسلات لاستخراج البتات المخفية بعد استخراج البتات الثنائية، يتم تجميعها في مجموعات من (8 بت) ومن ثم تحويل البتات إلى القيم الأصلية لإعادة بناء الصورة المخفية.

1.5 طريقة الاخفاء لخوارزمية MSD:-

- **المدخلات:** صورة الغلاف، CI (M,N)

M :هو عدد الصفوف. N: هو عدد الأعمدة. n: عدد صحيح اكبر من 0،(حجم مجموعة البكسلL:). عدد صحيح، 1< L،(حجم كتلة دفق الرسالة السرية الثنائية S).

- **المخرجات:** صورةstego، SI(M,N).

2.5 مثال على طريقة عمل الخوارزمية:

إذا كانت كتلة من صورة الغلاف (x_1, x_2, x_3)= (23,26,27) و s = 8، فيمكننا إيجاد وحدات البكسل المخفية (y_1, y_2, y_3) = (24، 26، 27) باستخدام مخطط إخفاء بيانات MSD.

- **الخطوة 1:** احسب

-

$$t=ef(x_1, x_2, \ldots, x_n)$$

$$t = \sum_{i=1}^{n} x_i \cdot (2^{(i-1)}) mod\ tn \qquad (5)$$

$$27 \bmod 11 = 183 \bmod 11 = 7\times 26 + 4 \times 23 + 2 \times 1$$

- **الخطوة 2:**

احسب الفرق $d = 8 - 7 = 1 = (001)_2$

http://www.doi.org/10.62341/amsz1803

- **الخطوة 3:** بما أن $d< 2^n$ فيتم تطبيق الحالة 2 فنحصل علي النتيجة (24، 26، 27)

يمكن للمُستقبل استعادة البيانات السرية باستخدام المعادلة(5)

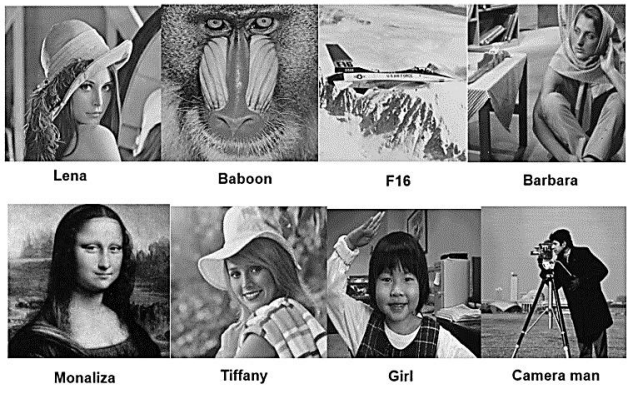
$$s= f(s)(24, 26, 27)$$

$$826+ 4 \times 27 \bmod 11 = 181 \bmod 11 = \times 24+2\times=1$$

بالإضافة إلى ذلك، ولتجنب مشكلة الفائض أو نقصان الفائض، يمكننا أولاً تعديل قيمة البكسل من 0 إلى 1 او من 255 إلى 254 عندما تكون قيمة البكسل 0 أو 255 على التوالي.

6. الجانب العملي

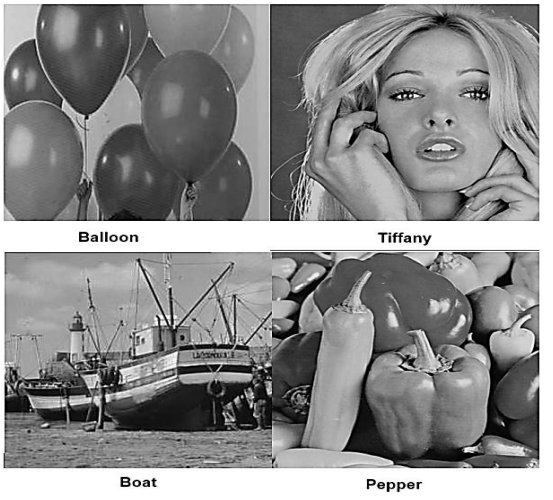
في تنفيذ الجانب العملي تم استخدام برنامج الماتلاب لتطبيق الخوارزمية، حيث تم استخدام أربع صور سرية بدرجات رمادية بنفس الحجم 512 × 512 بكسل؛ أما صور الغلاف فقد كانت بحجم 512 × 512 مرة وبحجم 1024 ×1024 مرة اخري. ومن ثم استخلاص النتائج من حيث نسبة الإشارة الي الضوضاء ومربع الخطأ وعدد الصور المستخدمة وكذلك نسبة استهلاك وقت المعالج والذاكرة المستخدمة. الشكل (2) يوضح الصور المستخدمة كغلاف.



الشكل.2 الصور المستخدمة كغلافcover images

أما الصور السرية فقد تم الحفاظ على خصائصها من حيث النوع (التدرج الرمادي) والحجم (512×512) الشكل (3) يوضح الصور السرية المستخدمة.

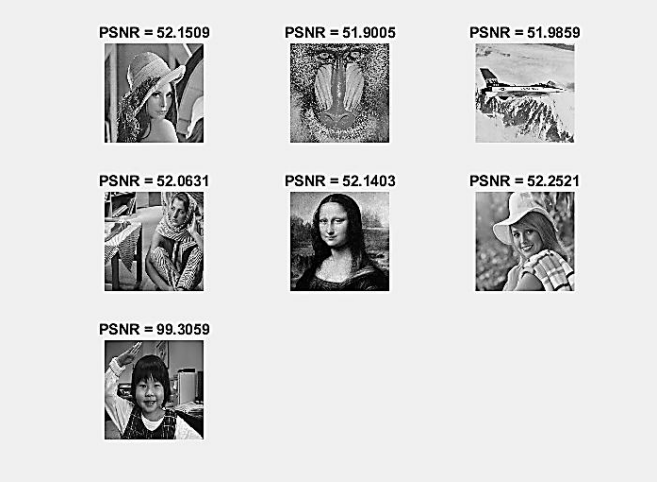
http://www.doi.org/10.62341/amsz1803



الشكل.3 الصور السرية المستخدمة

7. النتائج

يوضح الشكل (4) عينة من مخرجات التنفيذ التي تبين حساب المقاييس المطلوبة وذلك عند اختيار قيمة n=3 وصورة الغلاف بحجم512×512.



الشكل.4 عينة من مخرجات التنفيذ عند اختيار قيمة n=3

نلاحظ من مخرجات البرنامج في الشكل السابق انه تم استخدام عدد 7 صور من صور الغطاء لإخفاء الصورة السرية بحجم 512×512 كما نلاحظ أن الصورة الأخيرة لها PSNR أكبر لأنها لم تكن مضمنة بالكامل. كما أنMSE أقل نظرًا لأن عددًا أقل من وحدات البكسل قد تغيرت. يبين الجدولين (2،1) عدد الصور المستخدمة في حالات مختلفة من قيمةn.

http://www.doi.org/10.62341/amsz1803

الجدول.1 عدد الصور المستخدمة في حالة حجم الغلاف 512×51

المتغيرات	عدد البكسلات n من صورة الغلاف لاخفاء L من الصورة السرية			
	2	3	4	5
حجم البلوك L=n+1	3	4	5	6
عدد الصور المستخدمة N	6	7	7	7

الجدول.2.عدد الصور المستخدمة في حالة حجم الغلاف 1024×1024

المتغيرات	عدد البكسلات n من صورة الغلاف لاخفاء L من الصورة السرية			
	2	3	4	5
حجم البلوك L=n+1	3	4	5	6
عدد الصور المستخدمة N	2	2	2	2

يتم حساب عدد بلوكات الصورة السرية حسب المعادلات التالية:-

$$H = \left\lceil \frac{\text{حجم الصورة السرية}}{\text{حجم البلوك } L} \right\rceil \quad (6)$$

حيث L=n+1 ويتم أيضا حساب عدد صور الغطاء بالمعادلة التالية:

$$N = \left\lceil \frac{H}{\frac{S}{n}} \right\rceil \quad (7)$$

حيث أن: -

S= حجم صورة الغطاء .n= عدد البكسلات في كل كتلة من صورة الغطاء

الجدول (3) يبين النتائج المطلوبة في حالة الحجم 512×512 بينما الجدول (4) يوضح النتائج في حالة الحجم 1024×1024.

الجدول.3 النتائج في حالة حجم الغلاف 512×512

الجدول.4 النتائج في حالة حجم الغلاف 1024×1024

http://www.doi.org/10.62341/amsz1803

8. المناقشة

المقياس	المعدل	عدد البكسلات n لكل block L=n+1			
		2	3	4	5
PSNR (dB)	المستخدمة بالكامل	52.17	52.79	52.31	52.09
	المجموعة كاملة	52.96	58.88	52.61	52.33
MSE	المستخدمة بالكامل	0.45	0.44	0.41	0.40
	المجموعة كاملة	0.38	0.37	0.34	0.31
Time (Sec)	المستخدمة بالكامل	7.61	5.84	4.40	3.60
	المجموعة كاملة	6.80	5.03	4.18	3.42
Memory (MB)		480	484	487	491
Capacity (BPP)		1.16	1.15	1.099	1.20

من الجدول (3) والجدول (4)، نلاحظ أن لدينا متوسطان، الأول للمتوسطات بدون الصورة الأخيرة، بينما الثاني للمتوسطات مع الصورة الأخيرة التي لم يتم تضمينها بالكامل

المقياس	المعدل	عدد البكسلات n لكل block L=n+1			
		2	3	4	5
PSNR (dB)	المستخدمة بالكامل	54.17	53.79	53.25	52.82
	المجموعة كاملة	54.88	53.94	53.58	52.73
MSE	المستخدمة بالكامل	0.62	0.54	0.51	0.50
	المجموعة كاملة	0.42	0.41	0.41	0.42
Time (Sec)	المستخدمة بالكامل	4.61	3.77	2.92	2.02
	المجموعة كاملة	4.26	3.31	2.47	1.97
Memory (MB)		480	491	493	496
Capacity (BPP)		1.16	1.15	1.099	1.20

كما تم حساب النتائج أعلاه لجميع حالات n. لكلا الحجمين. نلاحظ ان النتائج لـ PSNR وMSE هي تقريبا نفسها لأن الخوارزمية MSD تقوم بتغيير أكثر من بكسل واحد في المجموعة بمقدار ±1، وهذا يعني أنه لا يعتمد على الحجم، وكذلك لسعة التضمين التي تم حسابها.

http://www.doi.org/10.62341/amsz1803

بالنسبة لاستهلاك الذاكرة، فإن استخدام صور غلاف 1024×1024 يستهلك ذاكرة أكبر من استخدام صور غطاء 512×512، حيث يتطلب استخدام حجم أكبر حجز مواقع أكبر في الذاكرة لحجم صورة المصفوفة.

أيضا بالمقارنة مع استخدام حجم صورة الغلاف 512×512 و1024×1024 ومن الجدولين السابقين نجد أنه عندما نستخدم حجم أكبر لصورة الغلاف، فإننا نستهلك وقتًا أقل. اما في حالة استخدام صور غلاف بحجم 512 × 512، فإننا نحتاج إلى المزيد من صور الغلاف ومن ثم المزيد من الوقت لمعالجة البيانات. من ناحية أخرى، لكلا الحجمين نحصل على نتائج متقاربة لمقاييس PSNR وMSE وسعة التضمين BPP.

9. الخلاصة:

من النتائج والمناقشة السابقة يتبين أن مميزات خوارزميةMSD صعوبة الاكتشاف بفضل توزيع البيانات على أكثر من بيكسل وتعديلها بشكل يعتمد على الأوزان بحيث يصعب اكتشاف البيانات المخفية أو طريقة التوزيع. كما أن التعديلات على الصورة تكون صغيرة للغاية، مما يحافظ على جودة الصورة دون أن يكون هناك اختلاف مرئي.

أيضا تتميز الخوارزمية بالمرونة، حيث يمكن اختيار حجم الكتلة nلإخفاء كميات مختلفة من البيانات حسب حاجة المستخدم. كما تبين أيضا ان زيادة حجم الغطاء يتطلب المزيد من الذاكرة. كما يتطلب وقتًا أقل. أيضا يمكن استخدام مجموعة منفصلة من n−pixel من صورة الغلاف لتضمين كتلL=n+1 من بتات الصورة السرية. حيث يمكن تغيير قيمة بكسل واحدة على الأقل في كل مجموعة بمقدار ±1.

10.المراجع:

[1]Cheddad, A., Condell, J., Curran, K., & Kevitt, P. M. (2010, October). Digital Image Steganography: Survey and Analysis of Current Methods. *Signal Processing*, pp. 727-752. Vol 90. No.3.

[2] Hegde, R., & S, J. (2015, July). Design and Implementation of Image Steganography by Using LSB Replacement Algorithm and Pseudo RandomEncoding Technique. International Journal on Recent and Innovation Trends in Computing and Communication, pp.4415 - 4420. Vol 3. No.7.

[3]Om-Essad M. Lamiles, Hajer A. Alaswed ” Analysis and Experimental Study of EMD and GEMDSteganographic Methods “.Libya Journal Applied For Science and Technology. LJAST .Volume 6. Issue 1 June 2019

http://www.doi.org/10.62341/amsz1803

[4] P. Kaur, H. Singh, A. Gupta and A. Girdhar, "An improved steganographic approach to diminish data modification for enhancing image quality," International Conference on Medical Imaging, mHealth and Emerging Communication Systems, pp. 329-333, 2014.

[5] أم السعد محمد الاميلس وفائزة إسماعيل الجروشي " استخدام الصور الرمادية للمقارنة بين طرق الإخفاء المعتمدة على قيمة البكسل و البت الأعلى أهمية Third " International Conference on Technical Sciences (ICST2020), 28-30 November 2020, Tripoli – Libya

[6]Wang, R. Z; Lin, C. F.; & Lin, J. C (2001, May). Image Hiding by Optimal LSB Substitution and Genetic Algorithm. Pattern Recognition, pp.671-683 .Vol 34.No 3.

[7]Jarno, M. (2006, May). LSB Matching Revisited. IEEE, Signal Processing Letters, pp. 285- 287. Vol 13 No.5.

[8]Zhang, X., & Wang, S. (2006, November). Efficient Steganographic Embedding by Exploiting Modification Direction. IEEE Communication Letters, pp. 781-783. Vol 12. No.7.

[9]Lee .C.F; Wang. Y & Chang. C (2007, August). A Steganographic Method with High Embedding Capacity by Improving Exploiting Modification Direction. Proceedings of the Third International Conference on Intelligent InformationHiding and Multimedia Signal Processing(IIHMSP07), pp.497-500. Vol 5.No.2.

[10] Kuo, W.-C., & Wang, C.-C. (2013, October). Data Hiding Based on Generalised Exploiting Modification Direction Method. The Imaging Science Journal,pp.484-490. Vol 61. No.10.

[11] Kuo, W.-C., Wang, C.-C., & Hou, H.-C. (2015, August). Signed Digit Data Hiding Scheme. Information Processing Letters, pp. 15-26. Vol 5. No.2.

[12] Chang, C.-C., Hu, Y.-C., & Lin, C.-C. (2016). Reversible shared data hiding based on modified signed digit EMD. Journal of Systems and Software, 119, 147–159. https://doi.org/10.1016/j.jss.2016.06.06

[13] Solak, S. (2020). High embedding capacity data hiding technique based on EMSD and LSB substitution algorithms. IEEE Access, 8, 166513–166524.

http://www.doi.org/10.62341/amsz1803

[14] Kuo, W.-C., Chen, Y.-H., & Chuang, C.-T. (2014, April). High-Capacity Steganographic Method Based on Division Arithmetic and Generalized Exploiting Modification Direction. Journal of Information Hiding and Multimedia Signal Processing, pp. 213-222. Vol 5. No.2.