خوارزمية متقدمة للتقاطع الهندسي بين المخروط والصور لإخفاء البيانات السرية

عبد المنعم العبدالله

قسم هندسة الاتصالات، كلية الهندسة الكهربائية والإلكترونية، جامعة حلب

الملخص

الإخفاء هو فن أو علم الاتصالات المخفية, والذي يدمج المعلومات السرية مع ملف غطاء (نص, صورة, صوت, فيديو) بحيث لا يثير شبهة المتنصت.

إن سعة الإخفاء مقيدة ومحدودة بحجم الصور الحاملة بالإضافة إلى وجود تعارض بين سعة الإخفاء وجودة الصورة المعماة, لذلك تبقى زيادة سعة الإخفاء مع تحسين جودة الصورة المعماة متغيرة, وهذا بالضبط جوهر بحثنا.

تعمل الخوارزمية المطورة على زيادة عدد نقاط تقاطع مستويات الخانة للصورة الأصلية مع الشكل الهندسي المخروطي ومن ثم تخزين الرسالة الأصلية ضمن هذه النقاط, فنحصل على الصورة المعماة, وذلك لزيادة سعة الإخفاء مع السعي للحفاظ على جودة صورة معماة معيارية, وقد تم بناؤها باستخدام بيئة الماتلاب, حيث تم دراسة سعة الإخفاء ومعاملات الجودة (MSE, PSNR), ومقارنة هذه النتائج مع نتائج التقاطع الهندسي للسطح المخروطي, والأشكال الهندسية.

الكلمات المفتاحية: الإخفاء, مخروط, هرم رباعي, كرة, سرية, مربع الخطأ المتوسط, نسبة الإشارة إلى الضجيج.

ورد البحث للمجلة بتاريخ 2016/10/12

وقبل للنشر بتاريخ 2017/1/15

Advanced Geometric Intersection Algorithm between Cone and Image for Hiding Secret Data

Abdulmonem Alabdalaa
Dept. of Communication Engineering, Faculty of Electrical & Electronic Engineering, University of Aleppo

Abstract

Steganography is the art or science of hidden communication that embeds secret data in public cover media as (text, image, audio, or video) not to arouse an eavesdropper's suspicion. The capacity is limited and restricted by the size of cover images. In addition, there is a trade-off between steganographic capacity and stego image quality (MSE, PSNR). Therefore, increasing steganographic capacity and enhancing stego image quality are still challenges, and this is the aim of this research.

The advanced algorithm tries to increase the number of intersection points (bit planes) of the original image with cone geometric shape and then the original message is stored at those intersection points, resulting in a stego-image, for increasing stego-capacity, in addition to trying to keep typical stego image quality.

We have implemented the technique in Matlab, and we have tested quality factors of (MSE, PSNR), in addition to stego capacity, then we have compared these results with that of the cone, sphere, and square pyramid and geometric shapes.

Keywords: Steganography, cone, square pyramid, sphere, Secret, MSE, PSNR.

Received 12/10/2016
Accepted 15/1/2017

1- الإخفاء وخصائصه وتقنياته:

يعرف الإخفاء بأنه إدخال المعلومات السرية في حوامل زائفة تبدو بريئة (رسائل غطاء) بطريقة لا يمكن من خلالها رؤية أو اكتشاف وجود المعلومات المخفية بالوسائل الإدراكية أو الإحصائية [1].

يجب توفر عنصرين هامين لإنجاز الإخفاء, ألا وهما المعلومات السرية المراد إخفاؤها, والملف الغطاء (الوسيط) الحامل للمعلومات السرية.

تتمثل الخصائص الأساسية لأنظمة الإخفاء في:

1- السعة: وهي عدد الخانات الأعظمي الممكن إخفاؤها في ملف الغطاء (الوسيط).

2- السرية (عدم الكشف): وهي استحالة اكتشاف المهاجم وجود رسالة مخفية ضمن الملف المعمى.

3- المتانة: مقاومة المعلومات المخفية لجميع أنواع الهجوم والقدرة على استرجاع وكشف العلامة المائية.

تطبيقات الإخفاء كثيرة منها:

1- الاتصالات السرية,

2- التجارة الإلكترونية,

3- العلامة المائية,

يتم تصنيف إخفاء المعلومات حسب معيارين:

1- نوع الملف الغطاء 2- طريقة الإخفاء المستخدمة (الحشر, الاستبدال, التوليد)

كما يتم تصنيف تقنيات إخفاء المعلومات إلى:

1- أنظمة الاستبدال,

2- تقنيات مجال التحويل,

3- الطيف المنتشر,

4- التقنيات الإحصائية,

5- التشويه,

6- توليد الغطاء.

أما تقنيات الإخفاء في الشبكات فتصنف إلى:

1- إخفاء المعلومات في المرفقات,

2- إخفاء المعلومات في النقل,

3- إخفاء المعلومات في عنونة الشبكة,

4- إخفاء المعلومات في بروتوكول صريح.

تتمثل هجمات الإخفاء بثلاثة أنواع:

1- الهجوم السلبي: تتم فيه مراقبة الاتصالات فقط بدون أي تدخل,

2- الهجوم الفعال: يتم من خلاله تعديل محتوى الملف المعمى,

3- الهجوم الخبيث: ينتحل فيه المهاجم شخصية أحد طرفي الاتصال.

2- دراسة مرجعية:

يوجد العديد من تقنيات الإخفاء فمثلاً قدم الباحث في [2] تقنية سهلة وذات انتشار واسع عن طريق استبدال الخانة الأقل أهمية LSB من كل بكسل للصورة (الملف الغطاء) بالبيانات السرية المراد إخفاؤها, إلا أن سريتها منخفضة جداً وسهلة الكشف وذات أماكن استبدال ثابتة, أما المرجع [3] فقد قدم تقنية لإخفاء البيانات الهامة عن طريق التحويل للمجال الترددي ومن ثم تنفيذ عملية إخفاء البيانات إلا أنها قابلة للكشف بالوسائل الإحصائية, بالإضافة إلى محدودية سعة الإخفاء, بينما تمكن الباحث في [4] من تقديم طريقة لإخفاء البيانات السرية عن طريق تقاطع شكل هندسي مخروطي (Cone) مع مستويات الخانة للصورة الحاملة (الغطاء), كما قدم الباحث في [5] طريقة لإخفاء البيانات السرية عن طريق تقاطع شكل هندسي أسطواني (cylinder) مع مستويات الخانة للصورة الحاملة (الغطاء), إلا أنه لم يتطرق إلى النتائج التي تم الحصول عليها, بالإضافة إلى تقديم الباحث في [6] طريقة لإخفاء البيانات الهامة عن طريق تقاطع شكل هندسي كروي (sphere) مع مستويات الخانة للصورة الحاملة وعرض نتائج سعة الإخفاء وجودة الصور المعماة التي حصل عليها, بالإضافة إلى تقديم الباحث في [7] طريقة لإخفاء البيانات السرية عن طريق تقاطع شكل هندسي هرم رباعي (Square Pyramid) مع مستويات الخانة للصورة

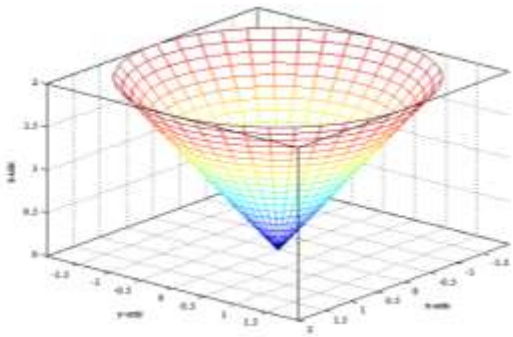
الحاملة وعرض نتائج سعة الإخفاء وجودة الصور المعماة التي حصل عليها ومقارنتها مع الأشكال الهندسية (الكروي, المخروطي).

إن من أهم خصائص الإخفاء هي كمية البيانات المخفية بالإضافة إلى جودة الصورة المعماة, وهذا ما تم العمل عليه في هذا البحث, حيث تم تطوير خوارزمية الإخفاء المعتمدة على التقاطع الهندسي بين الشكل الهندسي المخروطي ومستويات الخانة للصورة الغطاء على عدة مستويات, وذلك بزيادة عدد نقاط التقاطع لكل مقطع من مقاطع الشكل الهندسي المخروطي مع مستويات الخانة للصورة الرمادية الحاملة, مما ساهم في زيادة سعة الإخفاء مع الحفاظ على جودة صورة معيارية.

3- أهمية البحث وأهدافه:

تتجلى أهمية هذا البحث بتطوير تقنية إخفاء المعلومات السرية عن طريق تقاطع شكل هندسي مخروطي مع الصورة الحاملة, وذلك من خلال زيادة عدد نقاط التقاطع بين مقاطع السطح المخروطي ومستويات الخانة للصورة الغطاء, بهدف تأمين زيادة في سعة الإخفاء عن النتائج المقدمة سابقاً, مع العمل للحفاظ على جودة صورة معماة معيارية. تتميز هذه التقنية بسريتها العالية, من خلال عدم مقدرة المهاجم على اكتشاف الشكل الهندسي المستخدم (المخروط) في خوارزمية الإخفاء كما هو مبين في الشكل(1), ولزيادة السرية بشكل أكبر تم جعل السطوح الدائرية التابعة للمخروط والمتقاطعة مع مستويات الخانة للصورة على شكل قطوع ناقصة, بالإضافة إلى أنه إذا تمكن المهاجم من معرفة الشكل الهندسي المستخدم (مخروط), فإن محدداته تبقى مبهمة بالنسبة له, حيث أن (مركز المخروط, أنصاف أقطار سطوح القطوع الناقصة) تعد معلومات سرية خاصة بكل من المرسل والمستقبل, بالإضافة إلى عدد مستويات الخانة (Bit Planes) وعدد مقاطع سطح المخروط المستخدمة في الإخفاء هي معلومات سرية أيضاً, وهذه المعلومات إما أن تكون ثابتة لدى طرفي الاتصال, أو من الممكن ارسالها بملف مستقل عن ملف الصورة الحاملة للبيانات السرية, ليتمكن طرف الاستقبال من خلالها باستخلاص المعلومات السرية من الصورة الحاملة, كما تبرز أهمية البحث من خلال سرعة تنفيذ الإخفاء على الصورة وعدم اختلاف حجم الصورة

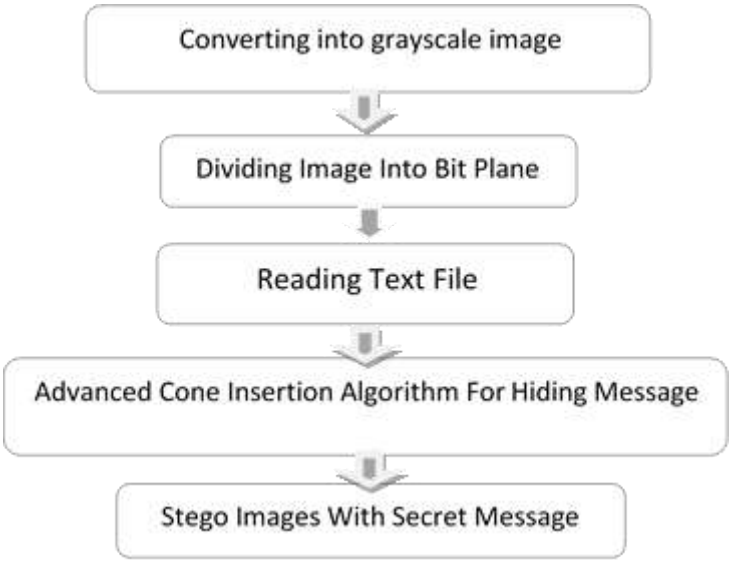
المعماة عن الصورة الأصلية, لأنها معتمدة على تقنية الاستبدال (المجال الفراغي), بالإضافة إلى توفير سعة إخفاء تصل إلى 13.7% من حجم الصورة الحاملة (الغطاء), وجودة صورة معماة PSNR تتراوح بين (20 – 40 dB) والتي تعد قيم معيارية حسب [8].



الشكل1: المخروط الذي يتم استخدامه في خوارزمية الإخفاء

4- بنية خوارزمية الإخفاء:

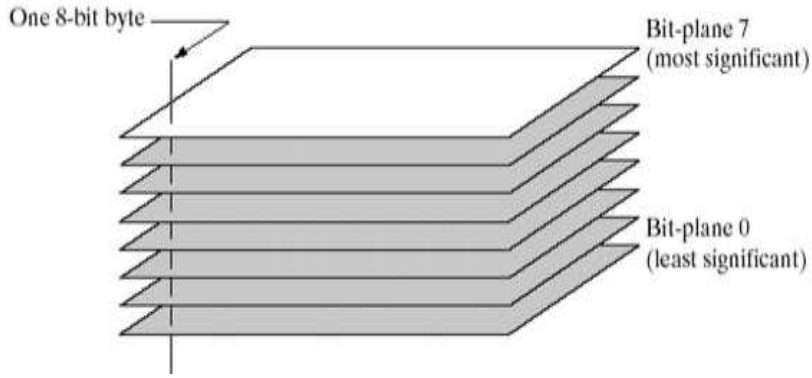
تعمل الخوارزمية المقترحة وفق الآلية المبينة في الشكل (2):



الشكل2: بنية الخوارزمية

تعتمد هذه الخوارزمية على تقنية الاستبدال (مجال فراغي), حيث يتم أولا إدخال الصور الملونة الحاملة (الغطاء) وتكون ذات تنسيق من نوع (*.jpg), ومن ثم

يتم تحويل الصورة المدخلة إلى صورة رمادية بأبعاد 256*256, حيث أن كل Pixel يمثل بـ 8Bits , وبالتالي حجم الصورة الرمادية Bits 524288 =8*256*256, وبعدها يتم تقسيم الصورة إلى عدد من مستويات الخانة (Bit planes Slicing) كما في الشكل (3), أي أن الـ (Bit Plane0) يحوي كل الخانات الأقل أهمية (LSB), والـ (Bit Plane1) يحوي كل الخانات الأقل أهمية الثانية, (Bit Plane7) يحوي كل ال الأكثر أهمية (MSB).



الشكل3: مستويات الخانة

وبعد قراءة المعلومات السرية من ملف نصي بامتداد (*.TXT), يتم تحويل كل محرف من النص السري إلى الشكل الثنائي وبثمانية خانات وتخزينها بشكل متسلسل ضمن مصفوفة, ليتم إدخال هذه المعلومات السرية الثنائية في نقاط تقاطع مستويات الخانة للصورة الرمادية مع الشكل الهندسي المعتمد (مخروط مطور) وعلى عدة مستويات, كما في المثال التالي:

لتكن نقاط التقاطع بين الشكل الهندسي المخروطي المطور والصورة الحاملة هي P4(115,95) ,P3(100,90), P2(90,80), P1(86,76), وهذه النقاط تحمل القيم اللونية التالية: P1=11100010, P2=11000111, P3=10011001, P4=11000110

أي أصبح تسلسل بيانات الصورة: 11100010110001111001100111000110

وفرضاً لدينا تسلسل النص السري:[1101011010111000]=M

وبعد استبدال خانات البيانات السرية بخانات بيانات الصورة, بالتسلسل وبالألوان المتقابلة, من الخانة الأقل أهمية (LSB) إلى الخانة الرابعة (الإخفاء هنا على أربعة مستويات من الخانة), يصبح تسلسل خانات بيانات الصورة كالتالي:

11101011 11000110 10011101 11000001

وبالنتيجة الصورة التي تحوي النص السري تدعى بالصورة المعماة (Stego-Image), وتكون بنفس حجم الصورة الأصلية.

يعرف الشكل الهندسي المستخدم (المخروط) من خلال مركزه (X0,Y0), ونصفي قطري القطع الناقص (a,b), وفق العلاقتين الرياضيتين التاليتين [9], حيث أن X يمثل رقم سطر بيكسل الصورة المتقاطع مع القطع الناقص, أما Y فيمثل رقم عمود بيكسل الصورة المتقاطع مع القطع الناقص:

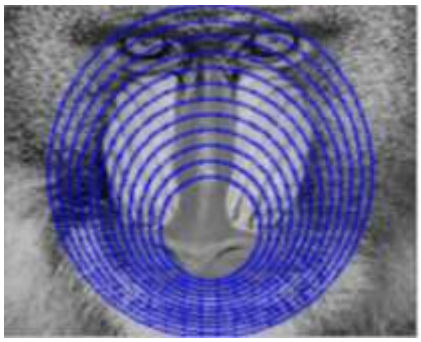
$$X = a*Cos\phi + X0 \quad (1)$$
$$Y = b*Sin\phi + Y0 \quad (2)$$

5- النتائج والمناقشة:

تعمل الخوارزمية المقترح تطويرها على زيادة نقاط تقاطع عدد من السطوح التابعة للمخروط (12 سطح) مع مستويات الخانة للملف الغطاء (الصورة الرمادية), حيث تم اعتماد هذا العدد من السطوح للمقارنة مع النتائج الواردة في [7], ولأنه أكبر عدد ممكن اجراء التقاطع بينه وبين الصورة الحاملة وفق البارامترات التالية المعتمدة, مع ملاحظة أن لكل شكل هندسي بارامتراته الخاصة والتي تحدد العدد الأعظمي للسطوح المتقاطعة للشكل المعتمد مع مستويات الخانة للصورة الحاملة, بالإضافة إلى أن هذا العدد يلعب دوراً في سعة الإخفاء وجودة الصورة المعماة, فزيادة هذا العدد تؤدي لزيادة سعة الإخفاء, ونقصان جودة الصورة المعماة (PSNR), إن مركز سطوح القطع الناقص العائدة للمخروط المطور متغير ويبدأ من البيكسل (128,128) من الصورة, وكذلك أطوال أنصاف أقطار سطوح القطع الناقص متغيرة حيث يمتد a1=128 pixels ويتناقص هذا الطول بمقدار 8pixels لنصف قطر القطع الناقص التالي وهكذا إلى سطح القطع الناقص الثاني عشر والذي يمتد طول ضلعه على طول a12=40 pixels, في حين يمتد b1=100pixels ويتناقص هذا الطول بمقدار

6pixels لنصف قطر القطع الناقص التالي وهكذا إلى سطح القطع الناقص الثاني عشر والذي يمتد طول ضلعه على طول b12=34pixels, ومن ثم يتم إدخال البيانات السرية ضمن نقاط التقاطع هذه, تم الاعتماد على صورتين (Lena, Baboon), يبين الشكلين (4,5) الصورتين الأصليتين بعد إيجاد نقاط التقاطع لإدخال البيانات السرية فيها, حيث تم إجراء التحليل باستخدام برنامج Matlab على /4/ مستويات من الخانة, /5/ مستويات من الخانة, /6/ مستويات من الخانة, و/8/ مستويات من الخانة, لدراسة سعة الإخفاء(Stego Capacity), وكذلك جودة الصورة المعماة (PSNR).

الشكل4: الصورة Lena قبل الإخفاء



الشكل5: الصورة Baboon قبل الإخفاء

5-1- سعة الإخفاء:

تعرف سعة الإخفاء بأنها كمية البيانات السرية المدخلة ضمن ملف الغطاء, وبما أن البيانات السرية لدينا هي خانات ثنائية (0,1), فتتحدد سعة الإخفاء من عدد الخانات الثنائية التي يتم إخفاؤها ضمن الصورة الرمادية (الغطاء).

وقد تم حساب سعة الإخفاء كنسبة مئوية من حجم الصورة الحاملة من خلال العلاقة التالية: النسبة المئوية للإخفاء = $\frac{\text{عدد الخانات الثنائية المخفية}}{\text{حجم الصورة الحاملة}} * 100$ (3)

5-1-1- سعة الإخفاء على أربعة مستويات:

تم هنا إخفاء البيانات السرية على أربعة مستويات من الخانة-0(Bit Planes Bit Plane3), حيث أظهرت النتائج سعة إخفاء تصل إلى حوالي 6.9% من حجم الصورة الحاملة (الغطاء), وبالمقارنة مع سعة الإخفاء للأشكال الهندسية (المخروطي,

الهرمي الرباعي, الكروي) على أربعة مستويات نجد أن الإخفاء المخروطي المطور يؤمن سعة الإخفاء الأكبر بين كل أنواع الإخفاء الهندسي كما هو مبين في الجدول (1), بالإضافة إلى أن الصور المعماة بطرق الإخفاء الهندسية لم تختلف بالرؤية عن الصور الأصلية كما هو مبين في الأشكال (6,7,8,9,10,11,12,13).

الشكل6: Lena بعد الإخفاء (Advanced Cone) على أربعة مستويات

الشكل7: Baboon بعد الإخفاء (Advanced Cone) على أربعة مستويات

الشكل8: Lena بعد الإخفاء (Cone) على أربعة مستويات

الشكل9: Baboon بعد الإخفاء (Cone) على أربعة مستويات

الشكل10: Lena بعد الإخفاء (Square Pyramid) على أربعة مستويات

الشكل11: Baboon بعد الإخفاء (Square Pyramid) على أربعة مستويات

الشكل12: Lena بعد الإخفاء (Sphere) على أربعة مستويات

الشكل13: Baboon بعد الإخفاء (Sphere) على أربعة مستويات

الجدول 1: سعة الإخفاء على أربعة مستويات [Bits]

Method / Image	Lena	Baboon
Proposed Advanced Cone	**36000**	**36000**
Cone [4]	**12800**	**12800**
Square Pyramid [7]	**17280**	**17280**
Sphere [6]	**34560**	**34560**

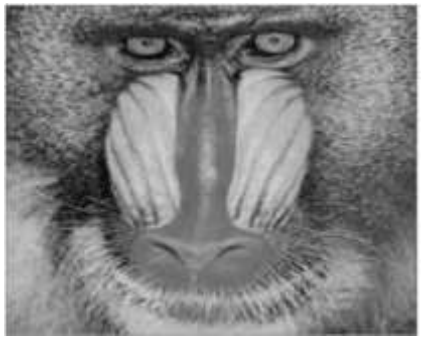
5-1-2- سعة الإخفاء على خمسة مستويات:

تم هنا إخفاء البيانات السرية على خمسة مستويات من الخانة (Bit Planes0-Bit Plane4), حيث أظهرت النتائج سعة إخفاء تصل إلى 8.6% من حجم الصورة الحاملة وبالمقارنة مع سعة الإخفاء للأشكال الهندسية (المخروطي, الهرمي الرباعي, الكروي) على خمسة مستويات نجد أن الإخفاء المخروطي المطور يؤمن سعة الإخفاء الأكبر بين كل أنواع الإخفاء الهندسية كما هو مبين في الجدول (2), كما أظهرت النتائج أن الصور المعماة بطرق إخفاء التقاطع الهندسي لم تختلف بالرؤية عن الصور الأصلية كما هو مبين في الأشكال (14,15,16,17,18,19,20,21).

الشكل14: Lena بعد الإخفاء (Advanced Cone) على خمسة مستويات

الشكل15: Baboon بعد الإخفاء (Advanced Cone) على خمسة مستويات

الشكل16: Lena بعد الإخفاء (Cone) على خمسة مستويات



الشكل17: Baboon بعد الإخفاء (Cone) على خمسة مستويات

الشكل18: Lena بعد الإخفاء (Square Pyramid) على خمسة مستويات

الشكل19: Baboon بعد الإخفاء (Square Pyramid) على خمسة مستويات

الشكل20: Lena بعد الإخفاء (Sphere) على خمسة مستويات

الشكل21: Baboon بعد الإخفاء (Sphere) على خمسة مستويات

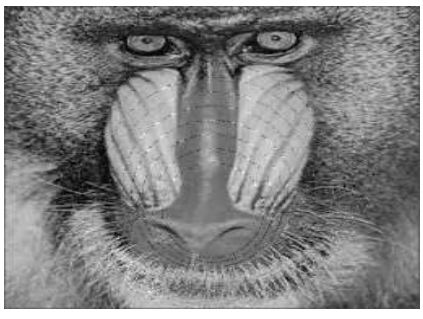
الجدول 2: سعة الإخفاء على خمسة مستويات [Bits]

Method / Image	Lena	Baboon
Advanced Cone	45000	45000
Cone	16000	16000
Square Pyramid	21600	21600
Sphere	43200	43200

5-1-3- سعة الإخفاء على ستة مستويات:

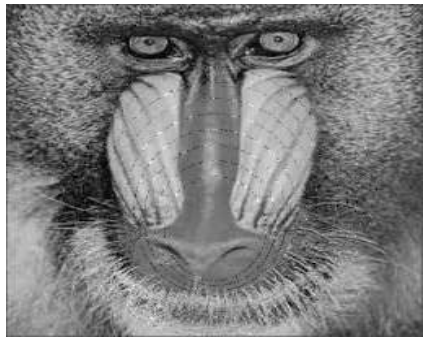
تم هنا إخفاء البيانات السرية على ستة مستويات من الخانة-0Bit Planes) (Bit Plane5, حيث أظهرت النتائج سعة إخفاء تصل إلى 10.3% من حجم الصورة الحاملة, وبالمقارنة مع سعة الإخفاء للأشكال الهندسية (المخروطي, الهرمي الرباعي, الكروي) على ستة مستويات نجد أن الإخفاء المخروطي المطور يؤمن سعة الإخفاء الأكبر بين كل أنواع الإخفاء الهندسية كما هو مبين في الجدول (3), إلا أن الصور المعماة بطرق الإخفاء الهندسية أبدت اختلافاً بالرؤية عند مقارنتها بالصور الأصلية (ظهور نقاط الادخال) كما هو مبين في الأشكال (22,23,24,25,26,27,28,29).

الشكل22: Lena بعد الإخفاء (Advanced Cone) على ستة مستويات



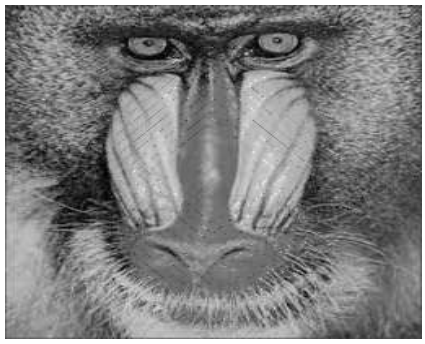
الشكل23: Baboon بعد الإخفاء (Advanced Cone) على ستة مستويات

الشكل24: Lena بعد الإخفاء (Cone) على ستة مستويات



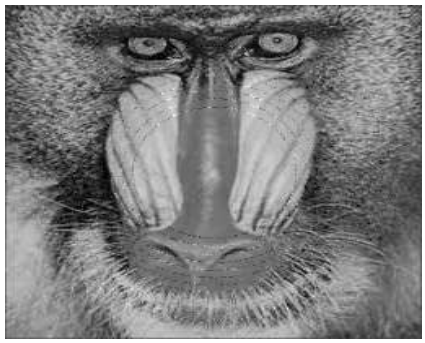
الشكل25: Baboon بعد الإخفاء (Cone) على ستة مستويات

الشكل26: Lena بعد الإخفاء (Square Pyramid) على ستة مستويات



الشكل27: Baboon بعد الإخفاء (Square Pyramid) على ستة مستويات

الشكل28: Lena بعد الإخفاء (Sphere) على ستة مستويات



الشكل29: Baboon بعد الإخفاء (Sphere) على ستة مستويات

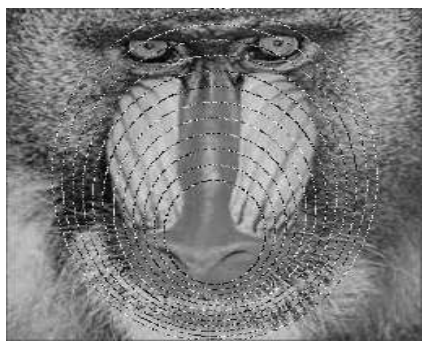
الجدول 3: سعة الإخفاء على ستة مستويات [Bits]

Method / Image	Lena	Baboon
Advanced Cone	54000	54000
Cone	19200	19200
Square Pyramid	25920	25920
Sphere	51840	51840

5-1-4- سعة الإخفاء على ثمانية مستويات:

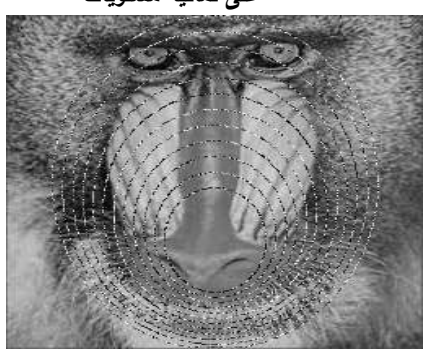
تم هنا إخفاء البيانات السرية على ثمانية مستويات من الخانة-0Bit Planes) (Bit Plane7, حيث أظهرت النتائج سعة إخفاء تصل إلى 13.7% من حجم الصورة الحاملة, وبالمقارنة مع سعة الإخفاء للأشكال الهندسية (المخروطي, الهرمي الرباعي, الكروي) على ثمانية مستويات نجد أن الإخفاء المخروطي المطور يؤمن سعة الإخفاء الأكبر بين كل أنواع الإخفاء الهندسية كما هو مبين في الجدول (4), بالإضافة إلى أن الصور المعماة بطرق إخفاء التقاطع الهندسية أبدت اختلافاً كبيراً بالرؤية عن الصور الأصلية كما هو مبين في الأشكال (30,31,32,33,34,35,36,37).

الشكل30: Lena بعد الإخفاء (Advanced Cone) على ثمانية مستويات



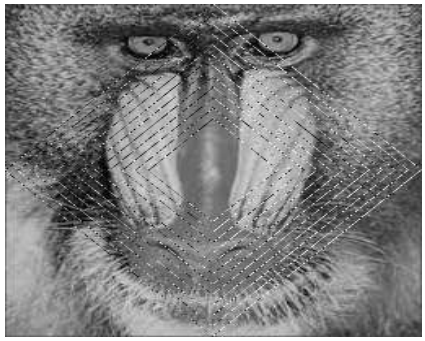
الشكل31: Baboon بعد الإخفاء (Advanced Cone) على ثمانية مستويات

الشكل32: Lena بعد الإخفاء (Cone) على ثمانية مستويات



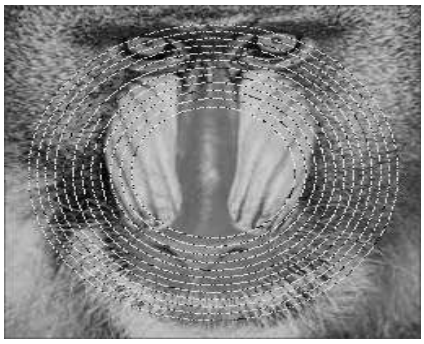
الشكل33: Baboon بعد الإخفاء (Cone) على ثمانية مستويات

الشكل34: Lena بعد الإخفاء (Square Pyramid) على ثمانية مستويات



الشكل35: Baboon بعد الإخفاء (Square Pyramid) على ثمانية مستويات

الشكل36: Lena بعد الإخفاء (Sphere) على ثمانية مستويات



الشكل37: Baboon بعد الإخفاء (Sphere) على ثمانية مستويات

الجدول 4: سعة الإخفاء على ثمانية مستويات [Bits]

Method / Image	Lena	Baboon
Advanced Cone	72000	72000
Cone	25600	25600
Square Pyramid	34560	34560
Sphere	69120	69120

5-2- جودة الإخفاء:

يتم حساب جودة الإخفاء عن طريق حساب نسبة الإشارة العظمى إلى الضجيج Peak Signal to Noise Ratio (PSNR) والتي تقاس بواحدة الديسبيل [dB], بالإضافة إلى مربع الخطأ المتوسط Mean Square Error (MSE), والمعرفان من خلال العلاقتين الرياضيتين التاليتين, حيث Xij يمثل قيمة البيكسل(i,j) في الصورة الأصلية و $\overline{Xij}$ يمثل قيمة البيكسل (i,j) في الصورة المعماة [10]:

$$MSE=\left[\frac{1}{256^2}\right]\sum_{i=1}^{256}{}'\sum_{j=1}^{256}\left(Xij-\overline{Xij}\right)^2 \quad (4)$$

$$\mathbf{PSNR = 10*log_{10}(\frac{256^2}{MSE})} \quad \mathbf{[dB]} \quad \mathbf{(5)}$$

5-2-1- جودة الإخفاء على أربعة مستويات:

تم هنا دراسة جودة الإخفاء (PSNR, MSE), بعد إخفاء البيانات السرية على أربعة مستويات من الخانة (Bit Plane0-Bit Plane3), حيث أظهرت النتائج جودة إخفاء PSNR > 36 dB وهي قيمة جودة متقاربة بالمقارنة مع نتائج جودة الإخفاء للأشكال الهندسية (المخروطي, الهرمي الرباعي, الكروي) على أربعة مستويات كما هو مبين في الجدول (5), بالإضافة إلى أن الصور المعماة لم تختلف بالرؤية عن الصور الأصلية كما هو مبين في الأشكال السابقة (6,7,8,9,10,11,12,13).

الجدول 5: جودة الإخفاء على أربعة مستويات PSNR [dB]

Method / Image	Lena	Baboon
Advanced Cone	36.35	36.18
Cone	37.03	36.95
Square Pyramid	36.28	36.15
Sphere	36.33	36.16

5-2-2- جودة الإخفاء على خمسة مستويات:

تم هنا دراسة جودة الإخفاء (PSNR, MSE), بعد إخفاء البيانات السرية على خمسة مستويات من الخانة (Bit Plane0-Bit Plane4), حيث أظهرت النتائج جودة إخفاء PSNR > 33 dB وهي قيمة متقاربة بالمقارنة مع نتائج جودة الإخفاء للأشكال الهندسية (المخروطي, الهرمي الرباعي, الكروي) على خمسة مستويات أيضاً كما هو مبين في الجدول (6), بالإضافة إلى أن الصور المعماة لم تختلف بالرؤية عن الصور الأصلية كما هو مبين في الأشكال السابقة (14,15,16,17,18,19,20,21).

الجدول 6: جودة الإخفاء على خمسة مستويات PSNR [dB]

Method / Image	Lena	Baboon
Advanced Cone	33.73	33.54
Cone	36.30	35.28
Square Pyramid	33.76	33.75
Sphere	33.76	33.64

5-2-3- جودة الإخفاء على ستة مستويات:

تم هنا دراسة جودة الإخفاء (PSNR, MSE), بعد إخفاء البيانات السرية

على ستة مستويات من الخانة (Bit Planes0-Bit Plane5), حيث أظهرت النتائج جودة إخفاء PSNR ~ 30 dB وقد تمت مقارنتها مع نتائج جودة الإخفاء للأشكال الهندسية (المخروطي, الهرمي الرباعي, الكروي) على ستة مستويات أيضاً كما هو مبين في الجدول (7), بالإضافة إلى ظهور نقاط إدخال البيانات السرية في الصور المعماة بشكل طفيف كما هو مبين في الأشكال السابقة (22,23,24,25,26,27,28,29).

الجدول 7: جودة الإخفاء على ستة مستويات [dB] PSNR

Method / Image	Lena	Baboon
Advanced Cone	**29.39**	**28.59**
Cone	**32.45**	**31.69**
Square Pyramid	**29.92**	**29.20**
Sphere	**29.43**	**28.68**

5-2-4- جودة الإخفاء على ثمانية مستويات:

تم هنا دراسة جودة الإخفاء (PSNR, MSE), بعد إخفاء البيانات السرية على ثمانية مستويات من الخانة (Bit Planes0-Bit Plane7), حيث أظهرت النتائج جودة إخفاء PSNR ~ 20 dB وقد تمت مقارنتها مع نتائج جودة الإخفاء للأشكال الهندسية (المخروطي, الهرمي الرباعي, الكروي) على ثمانية مستويات أيضاً كما هو مبين في الجدول (8), بالإضافة إلى ظهور نقاط إدخال البيانات السرية في الصور المعماة بشكل واضح كما هو مبين في الأشكال السابقة (30,31,32,33,34,35,36,37).

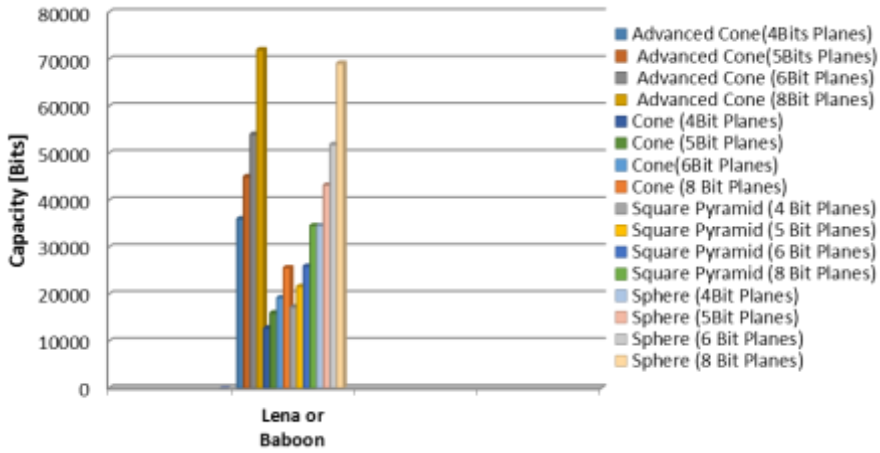
الجدول 8: جودة الإخفاء على ثمانية مستويات [dB] PSNR

Method / Image	Lena	Baboon
Advanced Cone	**19.15**	**18.87**
Cone	**21.94**	**22.75**
Square Pyramid	**19.44**	**19.18**
Sphere	**19.25**	**18.89**

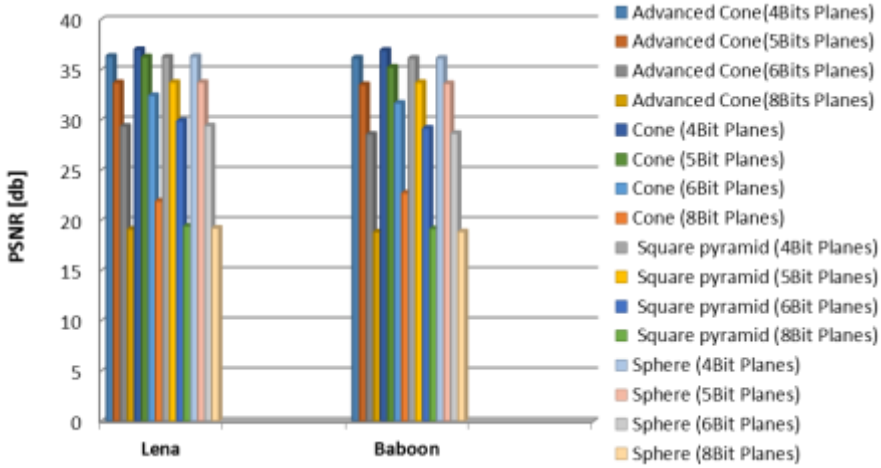
5-3- مخططات سعة الإخفاء وجودة الصور المعماة:

تم رسم مخطط يوضح سعة الإخفاء للخوارزمية المقترحة (المخروط المطور) نتيجة تطبيقها على الصورتين (Lena, Baboon) ومقارنتها مع نتائج سعة الإخفاء للأشكال الهندسية (المخروطي, الهرمي الرباعي, الكروي), حيث أظهر المخطط أن

سعة الإخفاء للشكل المخروطي المطور هي الأكبر من بين السعات, كما هو موضح في الشكل (38), بالإضافة إلى رسم مخطط ثانٍ يوضح جودة الإخفاء (PSNR) نتيجة تطبيق الخوارزمية المقترحة (المخروط المطور) على الصورتين (Lena, Baboon) ومقارنتها مع نتائج جودة الإخفاء للأشكال الهندسية (المخروطي, الهرمي الرباعي, الكروي), حيث أظهر المخطط أن نتائج جودة الإخفاء للأشكال الهندسية متقاربة في كل مستوى من مستويات الإخفاء ومحصورة بين (20 – 40 dB) كما هو موضح بالشكل (39).



الشكل38: سعة الإخفاء



الشكل39: جودة الإخفاء

6- الخلاصة

مما تقدم نستنتج أن الخوارزمية المطورة توفر سرية عالية, من خلال عدم مقدرة المهاجم على اكتشاف الشكل الهندسي المستخدم (المخروط) في خوارزمية الإخفاء, بالإضافة إلى أنه إذا تمكن المهاجم من معرفة الشكل الهندسي المستخدم, فإن محدداته تبقى مبهمة بالنسبة له, كما أن عدد مستويات الخانة (Bit Planes) وعدد مقاطع سطح المخروط المستخدمة في الإخفاء هي معلومات سرية أيضاً, بالإضافة لسعة الإخفاء تصل إلى 13.7% من حجم الصورة الأصلية الحاملة (الغطاء) وهذه السعة أكبر من السعة التي تم الحصول عليها بالتقاطع الهندسي المخروطي والتي وصلت إلى 5% من حجم الصورة الحاملة عند الإخفاء على ثمانية مستويات من الخانة, وجودة صورة معماة معيارية, وأفضل تلك النتائج من ناحية السعة والجودة هي عند الإخفاء على خمسة مستويات من الخانة (Bit Planes5) حيث أنها حققت توازن من ناحية السعة وجودة الصورة المعماة من بين النتائج التي تم الحصول عليها.

يمكن العمل على تطوير بعض خوارزميات التقاطع الهندسية المقدمة وذلك بغية زيادة سعة الإخفاء والمحافظة على جودة صور معماة معيارية ومقارنة نتائج الإخفاء مع النتائج التجريبية الحالية في دراسة قادمة.

المراجع

[1] T. Morkel.; J.H.P.Eloff.; and M.S. Olivier., 2007 – **An Overview of Image Steganography**. Information and Computer Security Architecture Research Group, Department of Computer Science, University of Pretoria, South Africa.

2] Life Science Journal., 2014 – **Steganography Technique for Embedding Secure Data into the Image Regions with Abrupt Changes**.http://www.lifesciencesite.com.

[3] Andreas Westfeld**.,** 2001 – **F5—A Steganographic Algorithm High Capacity Despite Better Steganalysis**. Technische Universit at Dresden, Institute for System Architecture.

[4]Viraj Sharadbhai Gandhi., 2010 – **Steganography Using Cone Insertion Algorithm and Mobile Based Stealth Steganography.** San Diego State University of Computer Science.

[5] Leezaben Ashokkumar Patel., 2010 – **Steganography Using Cylinder Insertion Algorithm and Mobile Based Stealth Steganography**. San Diego State University of Computer Science.

[6] Alabdalaa.; Salaho.; Tasqia., 2016 – **Data Steganography Algorithm Based on Geometric Intersection Between Sphere Surface and Image.** Res.Journal of Aleppo University (130).

[7] Alabdalaa.; Salaho.; Tasqia., 2016 – **Using Geometric Intersection Between Square Pyramid and Image for Hiding Secret Data.** Res.Journal of Aleppo University (131).

[8] Cole, E., 2003 – **Steganography and the Art of Covert Communication.** Indiana, John Wiley & Sons Inc.

[9] http://mathworld.wolfram.com/ Ellips.html.

[10] Chin-Chen Chang.; Yi-Hui Chen.; Chia-Chen Lin., 2008 – **A Data Embedding scheme for Color Images Based on Genetic Algorithm and Absolute Moment Block Truncation Coding.** Department of Information Engineering and Computer Science, Feng Chia University.