تغطية الصور المتدرجة الرمادي بملف فيديوي

المدرس المساعد رائد رافع عمر النعمة	المدرس المساعد فرقد حامد عبد الرحيم
الموصل/الكلية التقنية/ قسم هندسة تقنيات الحاسبات	

تغطية الصور المتدرجة الرمادي بملف فيديوي

المدرس المساعد رائد رافع عمر النعمة	المدرس المساعد فرقد حامد عبد الرحيم
الموصل/الكلية التقنية/ قسم هندسة تقنيات الحاسبات	

الملخص:

في هذا البحث تم استخدام ملف فيديو من نوع avi كوسط ناقل لإخفاء الصور المتدرجة الرمادي، وقد وفرت هذه الطريقة الدقة الشديدة في العرض والأمنية العالية في نقل البيانات. حيث تم تقطيع ملف الفيديو إلى مجموعة من الصور الثابتة، وبعدها تم تصميم خوارزميتين لإخفاء واسترجاع الصورة المتدرجة الرمادي. اهتمت خوارزمية الإخفاء بتحويل أي صورة متدرجة الرمادي إلى مجموعة من الرموز وخزنها داخل صور ثابتة لملف الفيديو. أما خوارزمية الإسترجاع فكانت عكس خوارزمية الإخفاء، حيث اهتمت هذه الخوارزمية بعملية استرجاع الصورة المتدرجة الرمادي من ملف الفيديو وإعادتها إلى صيغتها الأصلية. ولقد تمت عملية التغطية في ملف الفيديو بنجاح وحققت نسبة ١٠٠٪ في عملية إسترجاع البيانات المخزونة. تم تنفيذ الخوارزميتين باستخدام (MATLAP 7.6).

١. المقدمة Introduction:

ان استخدام الاتصالات السرية بواسطة رسائل مرمزة كان موضوع التطبيق العملي عبر التاريخ القديم والحديث فعند إرسال يوليوس قيصر رسائله إلى زعيمه كان يستخدم الشفرة الهجائية ليضمن عدم معرفة ما في الرسالة عند وقوعها في أيدي العدو.

وفي الحروب الحديثة تم استخدام الرموز والشفرات لضمان عدم تسرب المعلومات السرية إلى العدو، فضلا عن استعمال الرموز والشفرات من قبل الوكالات الأمنية لعدد من الحكومات والجيش والسلك الدبلوماسي لغرض إجراء الاتصالات. وهناك أيضا استعمالات أخرى، حيث هناك عدد كبير من الاتصالات التجارية ترسل عن طريق السلك أو أي وسط ناقل أخر على هيئة رموز لتقليل كلفة وحجم الرسائل [١].

لا يخفى بأن هنالك بحوث اهتمت بعملية تغطية بيانات نصية داخل بيانات نصية اخرى[٢]، وبحوث أخرى اهتمت بعملية تغطية بيانات نصية بداخل بيانات صورة نـــوع BMP [١]. هناك بعض المصادر التي تكلمت عن الإخفاء في مجال الفيديو عن طريق الوصول إلى الاطارات (frames) المكونة لملف الفيديو [٣] أو حتى المكونة لملف كليب VideoClip [٤]. في هذا البحث تم الاهتمام بتطوير عملية تغطية الصورالمتدرجة الرمادي بداخل ملف فيديوي بعد تقطيعه إلى صور، فهو تطوير للمصادر السابقة حيث أنه فتح آفاق لتغطية البيانات لأنواع أخرى من الصور.

٢. نظام التغطية Steganography:

كلمة (Steganography) مشتقة من اللغة الإغريقية وتتألف من مقطعين (Steganos) وتعني مغطاة أو سرية و(Graphy) وتعني الكتابة أو الرسم وهما معا يعنيان مصطلح الكتابة المغطاة (covered writing) [٥]، ويمكن تعريف الـ(Steganography) على أنه علم وفن الاتصال بطريقة تخفيمعلومات ضمن الاتصال أي نقل البيانات خلال بيانات أخرى تستخدم كمضيف (Host) أو حامل (Carrier) غير مؤذية كناقلات لتلك البيانات وبطريقة لا تسمح لأي عدو أو مراقب بان يكتشف أن هناك بيانات سرية [٦]. والإخفاء يهتم بسرية محتويات الرسالة إضافة إلى تحقيق سرية الاتصال وعندما يشك المتطفل بوجود معلومات مخفية فأنه يحاول أن يفك أو يدمر أو يغير الرسالة ثم يرسلها إلى المستلم الذي يعلم كيف يفسرها.

ستيكانوكرافي يعني حرفيا (الكتابة المغطاة) وتعنى بإخفاء الرسائل السرية ضمن رسالة أخرى تبدو غير مؤذية أو ناقل (Carrier) يمكن أن يكون الناقل أي شيء يستخدم لنقل المعلومات، متضمنا مثلا خشب أو لوحة أقراص، كعوب أحذية مجوفة، صور مطبوعة، صور صغيرة جدا أو ترتيبات كلمة [٢]. تتضمن النواقل الرقمية البريد الألكتروني (E-Mail)، الصوت (Audio)، الصور والرسائل الفيدوية [٧].

٣ـ الإخفاء في ملفات الفيديو الرقمية Hiding in Video Files

كما ذُكِر في الفقرة السابقة، هناك ملفات عديدة في الحاسوب من الممكن استخدامها كوسط لإخفاء الرسالة السرية ومن هذه الأوساط هي الصور الثابتة التي يتألف منها ملف الفيديو والمعروفة بالـ (frames) بذلك يمكن إخفاء المعلومات في الصور، فلإخفاء المعلومات يتم تضمين الرسالة من خلال اختيار مكان الضوضاء والتي لا تلفت النظر حيث يكون هناك اختلاف في اللون الطبيعي في هذه المناطق بكثرة.

بصورة عامة فان الحاسوب يتعامل مع ملف الفيديو على أنه مجموعة من الصور. ويتعامل أيضا مع الصورة على أنها منظومة ثنائية الأبعاد كل موقع فيها يمثل نقطة أو ما يعرف بالـ(Pixel) وهي أصغر وحدة لتمثيل موقع معين على الشاشة، وكلما زاد عدد هذه الوحدات الصورية (Pixels) ضمن حدود ثابتة ازداد تقارب هذه الصورة من الواقع في تحسس العين البشرية لحقائق هذه الصورة وهذا ما يسمى بـ(Resolution)، والتجمع لهذه النقاط بقيمها الخاصة من الألوان يدعى بـRGB وهي مختصر (Red, Green, Blue) الذي يكون لنا الصورة المرئية بحيث يمكن للعين المجردة إدراكها ، فلتمثيل كل نقطة من نقاط المصفوفة يكون من خلال استخدام ثلاث من الوحدات الخزنيه أو ما يدعى بالبايت، حيث يمكن لنا من الألوان الرئيسية

الثلاث أن نحصل على مزيج لوني حيث يخصص بايت واحد لكل لون من الألوان[٨].

إن الصور التي تتكون من ثمانية أرقام ثنائية لكل وحدة صورية للألوان الأساسية تمثل شدة الإضاءة في تلك النقطة اعتمادا على الألوان الأساسية (RGB). لذلك استُخدمت شدة كل لون من الألوان الأساسية لكل وحدة صورية كحاوٍ أو موقع خزن للرسالة، وقد رُمِّزت معلومات الرسالة إلى أرقام عشرية ثم خُزنت بإضافة كل رقم عشري من الرسالة إلى الرقم العشري الأقل أهمية من شدة اللون. حيث أن الأرقام العشرية الأخرى تحتوي على معلومات كافية لتمثيل اللون الصحيح لتلك الوحدة الصورية، وعند تغيير الرقم العشري الأقل أهمية لا يؤثر ذلك على الصورة بشكل ملحوظ.

٤ـ الطريقة المقترحة Suggested Method

قدمت هذه الطريقة مسار جديد في الستيكانوكرافي. حيث استخدمت ملف فيديو نوع avi كناقل صورة متدرجة الرمادي. ولهذه الطريقة ميزات عديدة، فهي فتحت طريق لتغطية البيانات لصور نوع BMP متدرجة الرمادي داخل وسط فيدوي، وفتحت طريقا آخر لتغطية عدد من الصور - أي كمية كبيرة من البيانات- بدلا من تحديد حجم البيانات المخزونة بحجم وسط صغير ناقل، كما استفادت هذه الطريقة من عملية تقطيع ملف الفيديو إلى مجموعة من الصور الثابتة والقيام بخزن البيانات في مصفوفات الألوان الرئيسية الثلاثة التي تشكل ألوان الصورة مما أتاح مساحة خزنية أكبر للصور التي تحوي على تدرج لوني واحد (الصور ذات التدرج الرمادي).

٤. ١ خوارزمية إخفاء الرسالة Message Hiding Algorithm

مرت عملية إخفاء الرسالة داخل ملف الفيديو بالخوارزمية التالية:

الخطوة الأولى: إدخال الصورة المتدرجة الرمادي.

الخطوة الثانية: فك بيانات الصورة إلى أرقامها العددية العشرية بحيث كل pixel يقابله ثلاثة أرقام عددية عشرية.

الخطوة الثالثة: تقطيع ملف الفيديو إلى صور ثابتة (frames).

الخطوة الرابعة: تصفير العمود ذو المرتبة العشرية الأدنى - وهو العمود الذي يمثل رقم الآحاد - لكل رقم في مصفوفة الألوان الرئيسية (الأحمر، الأزرق والأخضر)، وبحسب المعادلات التاليه رقم ١ ، ٢ و ٣:

$$mov_{f,i,j,1}=mov_{i,1}-mod(mov_{i,1}/10) \quad \ldots\ldots (1)$$

$$mov_{f,i,j,2}=mov_{i,2}-mod(mov_{i,2}/10) \quad \ldots\ldots (2)$$

$$mov_{f,i,j,3}=mov_{i,3}-mod(mov_{i,3}/10) \quad \ldots\ldots (3)$$

حيث:

mov هي مصفوفة الألوان الرئيسية

f صورة ملف الفيديو الثابتة *frame*

i عداد صفوف صورة ملف الفيديو الثابتة

j عداد أعمدة صورة ملف الفيديو الثابتة

mod إيعاز إقتصاص عدد الآحاد (باقي القسمة)

الخطوة الخامسة: من المعلوم أن الصورة المتدرجة الرمادي تتألف من أرقام تتراوح بين ٠-٢٥٥، لهذا يتم تقسيم هذه الأرقام العشرية إلى ثلاثة مراتب، كل مرتبة تخزن بداخل مصفوفة ثلاثية، حسب المعادلات التاليه رقم ٤ ، ٥ ، ٦ ، ٧ و ٨:

$$y_{i,j,1}=x_{i,j}-mod(x_{i,j}/100))/100 \quad \ldots\ldots (4)$$

$$x_{i,j}=x_{i,j}-y_{i,j,1}*100 \quad \ldots\ldots (5)$$

$y_{i,j,2}=(x_{i,j}-mod(x_{i,j}/10))/10$ ..... (6)

$x_{i,j}=x_{i,j}-y_{i,j,2}*10$ ..... (7)

$y_{i,j,3}=x_{i,};$ ..... (8)

حيث:

x هي مصفوفة الصورة المتدرجة الرمادي

y هي المصفوفة الناتجة من خزن أرقام المراتب الثلاثة للتدرج الرمادي

i عداد صفوف المصفوفة

j عداد أعمدة المصفوفة

x مصفوفة الأرقام المرمزة للرسالة

mod إيعاز إقتصاص عدد الآحاد (باقي القسمة)

الخطوة السادسة: القيام بحشر الأرقام الترميزية للصورة المتدرجة الرمادي بالمرتبة الأدنى التي تم تصفيرها في الخطوة الرابعة حسب المعادلة التالية رقم ٩:

$mov_{f,i,j,k}=y_{i,j,k}+ mov_{f,i,j,k}$ ..... (9)

حيث:

mov هي مصفوفة الألوان الرئيسية

y هي المصفوفة الناتجة من خزن أرقام المراتب الثلاثة للتدرج الرمادي

f صورة ملف الفيديو الثابتة *frame*

i عداد صفوف المصفوفة

j عداد أعمدة المصفوفة

k عداد من ١ إلى ٣

الخطوة السابعة: إعادة دمج وتجميع ملف الفيديو بعد إخفاء الصورة فيه.

٤. ٢ خوارزمية إسترجاع الرسالة Message Recovery Algorithm

مرت عملية إسترجاع الرسالة من ملف الفيديو بالخوارزمية التالية:

الخطوة الأولى: تقطيع ملف الفيديو إلى صور ثابتة (frames).

الخطوة الثانية: القيام بسحب الأرقام الترميزية للصورة المتدرجة الرمادي من المرتبة الأدنى لكل رقم في مصفوفة الألوان الرئيسية حسب المعادلة التالية رقم ١٠:

$$z_{i,j,k}=mod(mov_{f,i,,j,k}/10) \quad \text{.....(10)}$$

حيث:

mov هي مصفوفة الألوان الرئيسية

z هي المصفوفة الناتجة من إسترجاع أرقام المراتب الثلاثة للتدرج الرمادي

f صورة ملف الفيديو الثابتة *frame*

i عداد صفوف المصفوفة

j عداد أعمدة المصفوفة

k عداد من ١ إلى ٣

mod إيعاز إقتصاص عدد الآحاد (باقي القسمة)

الخطوة الثالثة: إعادة تجميع رموز الصورة المتدرجة الرمادي إلى ثلاثة أرقام ليقابل كل منها قيمة الـ pixel حسب المعادلة التالية رقم ١١:

$$X_{i,j}=z_{i,j,1}\times 100+z_{i,j,2}\times 10+z_{i,j,3} \quad \text{.....(11)}$$

حيث:

X تمثل الأرقام المرمزة للصورة المتدرجة الرمادي

z تمثل المصفوفة الناتجة من إسترجاع أرقام المراتب الثلاثة للتدرج الرمادي

i يمثل عداد صفوف المصفوفة

j يمثل أعمدة المصفوفة

الخطوة الرابعة: إستعادة وعرض الصورة حسب رموزها من الأرقام المسترجعة في الخطوة السابقة.

الخطوة الخامسة: التأكيد إعادة دمج وتجميع ملف الفيديو بعد سحب البيانات منه.

٥ـ عرض النتائج The Results

طبقت عملية الاخفاء على عدة صور متدرجة الرمادي نوع BMP. حيث تم إدخال الصورة من ملف خارجي إلى البرنامج. ولغرض قياس كفاءة الإخفاء، تم استخدام مقياس قمة نسبة الاشارة الى الضوضاء Peak Signal to Noise Ratio (PSNR)) والتي تقيس مدى دقة الاخفاء وإمكانية عدم تمييز الصورة المخفية في ملف الفيديو بالعين البشرية. بالنسبة لاخفاء الصور مقياس الدقة يتضمن حساب مربع الخطأ الذي يمكن ايجاده من المعادلتين التاليتين [٩]:

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(F_{ij} - G_{ij})^2 \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (12)$$

$$PSNR = 10\,Log_{10}\frac{L^2}{MSE} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (13)$$

حيث:

MSE حساب مربع الخطأ (Mean Spuare Error)

M,N هما الصف والعمود بالنسبة للصورة الغطاء

F_{ij} هي الوحدة الصورية من الصورة الغطاء قبل الاخفاء

G_{ij} هي الوحدة الصورية من الصورة الغطاء بعد الاخفاء

L هي مستوى قمة الاشارة.

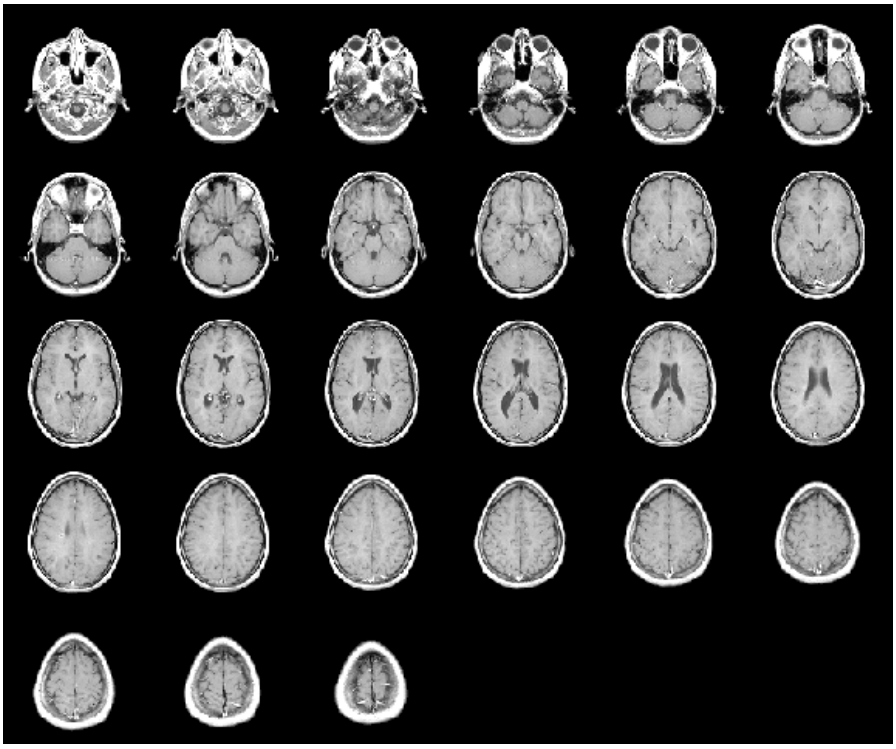
الجدول (١) يوضح قيمة MSEوPSNR بعد تطبيق عملية الاخفاء على ملف الفيديو لعدة صور متدرجة الرمادي، ولقد رتبت تصاعديا حسب حجم الإخفاء.

Text Order	Included pixels	PSNR
1	16384	38.8993
2	32768	44.3313
3	49152	48.3594
4	65536	50.7761

جدول (١)

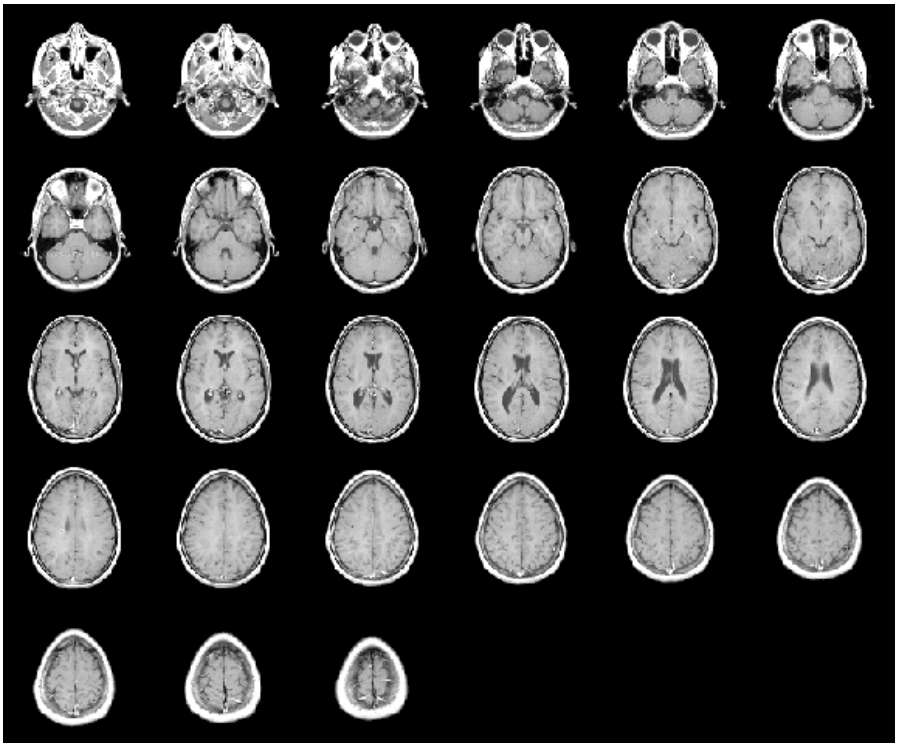
مقياس MSE و PSNR لمصفوفة صور ثابتة لملف الفيديو ولعدة صور

الواضح من الجدول (١) انه بزيادة حجم الصور المخفية تزداد قيمة PSNR ولكن كلما زاد الحجم قلت نسبة الزيادة مما يدل على كفاءة الخوارزمية المستخدمة في الاخفاء . وكذلك لا يمكن لأي شخص تمييز وجود صورة مخفية داخل ملف الفيديو. والأشكال التالية (١ و ٢) توضح ٢٧ صورة ثابتة (Frame) يتكون منها ملف الفيديو (والذي يمثل حركة الرنين المغناطيسي لدماغ الإنسان) مرتبة أفقيا بحسب تسلسل عرضها قبل إخفاء صورة فيها.



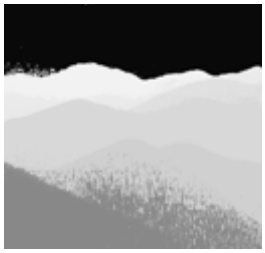
شكل رقم (١)

صور ملف الفيديو قبل عملية إخفاء صورة

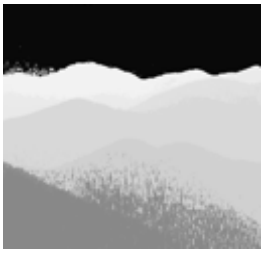


شكل رقم (٢)
صور ملف الفيديو بعد عملية إخفاء صورة

الشكلان السابقان أظهرا عدم وجود أي إختلاف ظاهر بالعين المجردة قبل إجراء عملية الإخفاء وبعدها. ولا يخفى أن حركة ملف الفيديو ستشكل عائقا أكبر لتمييز أي إختلاف - رغم عدم ظهوره - مما يعطي أمنية أكبر لنقل البيانات المخفية. الشكل (٣) يبين نماذج لصور متدرجة الرمادي تم إخفاؤها داخل ملف الفيديو واسترجاعها بنجاح تام وصل تقريباً ١٠٠٪.



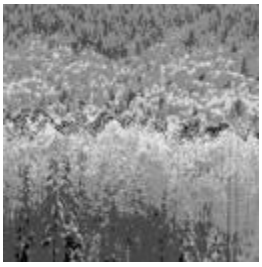
(a)



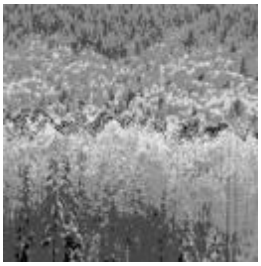
(b)

(c)

(d)



(e)



(f)

شكل رقم (٣)

نماذج لصور متدرجة الرمادي قبل وبعد عملية الإخفاء بداخل ملف الفيديو:

(a,c,e) قبل عملية الإخفاء

(b,d,f) بعد عملية الإخفاء

□

٦ـ الاستنتاجات Conclusions

قدم هذا البحث مسار جديد في الستيكانوكرافي حيث استخدم ملف فيديو كناقل لصور سرية، وتم من خلال هذا البحث التوصل إلى الكثير من النتائج المفيدة:

- فقد فتح الطريق لتغطية كمية كبيرة من البيانات بدلا من تحديد حجم البيانات المخزونة بحجم الصورة الناقلة.
- كما استفاد البحث من الإيعازات الجاهزة في برنامج الـ MATLAB بعملية تقطيع ملف الفيديو إلى مجموعة من الصور الثابتة والقيام بخزن البيانات في مصفوفة الألوان الرئيسية.
- إستخدام الألوان الرئيسية الثلاث التي تشكل ألوان الصورة في عملية الإخفاء وفر مساحة خزنية أكبر من إستخدام تدرج لوني واحد فقط.
- يمكن الإستفادة من المساحة الخزنية الكبيرة التي يوفرها ملف الفيديو لإخفاء بيانات ذات حجم أكبر.
- حركة ملف الفيديو ستشكل عائقا أكبر لتمييز أي إختلاف مما يعطي أمنية أكبر لنقل البيانات المخفية.
- مقياس دقة الإخفاء أثبت كفاءة الخوارزمية المستخدمة.
- بالإمكان إجراء تغطية لبيانات تتكون من أرقام عشرية ولا يشترط تحويلها إلى بيانات رقمية.

Abstract

In this research video file type avi is used to hide gray-scale images. This method offered high accuracy and secure for data transitions. It started by extract the fixed pictures (frames) from video file. Then two algorithms were adopted to implement the steganography process. The first algorithm concerns about converting the gray-scale image into corresponding codes, then store these codes inside the frame on video file. The second algorithm concerns about inverse the whole process of the first algorithm. Both

algorithms attained 100% success for data covering process and data getting back process. The steganography method applied in this work in Matlab environment version 7.6.

المصادر:

References

[١] شهد عبدالرحمن، ايلاف اسامة، "تطبيق نظام التغطية على الصور الملونة من نوع (BMP)"، المؤتمر العلمي الأول لتقانة المعلومات، كلية علوم الحاسبات والرياضيات/جامعة الموصل، ٢٢-٢٣ كانون الأول ٢٠٠٨.

[٢] د. دجان بشير، د.أحمد سامي، ياسين حكمت، "الإخفاء في النص باستخدام ميزة تكامل البيانات"، المؤتمر العلمي الأول لتقانة المعلومات، كلية علوم الحاسبات والرياضيات/جامعة الموصل، ٢٢-٢٣ كانون الأول ٢٠٠٨.

[3] Aelphaeis M., "Steganography FAQ", Zone-H Unrestricted Information, © Copyright Zone-H.Org 2006.

[4] Doërr, G. and J.L. Dugelay, "A guide Tour of Video Watermarking" Signal Processing: Image Commun., 18: 263-282. DOI: 10.1016/S0923-5965(02)00144-3, 2003.

[5] Mohammed A., "Image Steganography by Mapping Pixels to Letters", Journal of Computer Science 5 (1): 33-38, 2009, ISSN 1549-3636.

[6] R. Sridevi, Dr. A. Damodaram, Dr. Svl. Narasimham, "Efficient Method Of Audio Steganography By Modified Lsb Algorithm And Strong Encryption Key With Enhanced Security", Journal of Theoretical and Applied Information Technology, 2009.

[7] Krzysztof S., Igor M., Wojciech M., "Steganographic Routing in Multi Agent System Environment", Journal of Information Assurance and Security 2 (2007) 235-243.

[8] The MathWorks Inc., "Image Processing Toolbox For Use with MATLAB", Ver.7.6, 2008, MA, USA.

[9] Qi, Hairong; Snyder, Wesley E. & Sander, William A., 2002; "Blind Consistency-Based Steganography for Information Hiding in Digital Media". Multimedia and Expo, 2002. ICME '02. Proceedings. 2002 IEEE International Conference on Vol. 1, p.: 585- 588.