P- ISSN 1991-8941 , E-ISSN 2706-6703
2012 ,(6), (2) :13-19

(*JUAPS*) **مجلة جامعة الانبار للعلوم الصرفة**

Open Access

تقنية تكميم اتجاهي جديدة للكتابة المغطاة في JPG

أحمد سامي نوري **أنسام أسامة عبد المجيد**

جامعة الموصل - كلية علوم الحاسوب والرياضيات

معلومات البحث:
تاريخ التسليم: ٠٠/٠٠/٠٠
تاريخ القبول: ٠٠/٠٠/٠٠
تاريخ النشر: ٩/ ١٢ / ٢٠١٢
DOI: 10.37652/juaps.2012.63372

الكلمات المفتاحية:
تقنية تكميم اتجاهي ، الكتابة المغطاة ، JPG.

الخلاصة:

يهدف البحث إلى تصميم وتنفيذ خوارزمية جديدة للكتابة المغطاة في الصور الملونة ضِمن مجال الكبس باستخدام خوارزمية التكميم الاتجاهي Vector Quantization (VQ)، كون الملف المكبوس يعد غطاءً أمناً للبيانات المضمنة ويُجنّب إثارة انتباه الأشخاص غير المخولين، ويوفر كلاً من كلفة وزمن النقل والخزن. وتهدف الخوارزمية إلى زيادة كمية سعة التضمين مع المحافظة على جودة الصورة، فضلا عن تقليل زمن عملية الاستخلاص. الخوارزمية المقترحة نُفِّذَت باستخدام Matlab 2009a، واعتمدت في تضمين البيانات في كل فهرس على باقي قسمته على ٤ وعلى مفتاح سري مشترك بين الطرفين، كما استَخدمت صوراً رمادية وملونة بأبعاد مختلفة للامتداد (JPG) بعد كبسها لتكون غطاءً للبيانات السرية التي كانت نصا أو صورة. تبين من البحث أن الخوارزمية المقترحة قد حافظت على جودة عالية للصورة على الرغم من سعة التضمين العالية التي وصلت إلى استيعاب حجم الغطاء بالكامل، كما أن عدم الحاجة لوجود دليل الصورة لاستخلاص البيانات في الخوارزمية قلل زمن الاستخلاص وبشكل كبير.

المقدمة

نتيجة التطور الكبير في تقنيات الشبكات أصبح بإمكان الكثيرين الاتصال مع بعضهم البعض بسهولة وبسرعة عبر الانترنيت. ولأن الإنترنيت بيئة عامة ومفتوحة فبإمكان أي شخص غير مخول مراقبة معلومات متناقلة بين أي طرفين واعتراضها أو الحصول عليها؛ لذا فإن أهمية توفير الأمنية لتلك المعلومات تتزايد يوما بعد يوم للحفاظ على سريتها [١].

هناك تقنيتان لتوفير الأمنية للمعلومات المتناقلة وهما التشفير (Encryption) والكتابة المغطاة (Steganography) ، إذ يهدف التشفير إلى إعادة صياغة البيانات بواسطة مفتاح التشفير بحيث تبدو غير مفهومة لكنها لا تخفي حقيقة وجود اتصال سري بين طرفين مما دفع الكثيرين نحو استخدام الكتابة المغطاة؛ إذ أنها تقنية تُضِمّن بيانات سرية داخل بيانات أخرى بصورة لا يمكن ملاحظتها مما يخفي حقيقة وجود بيانات سرية متناقلة [٢].

الكتابة المغطاة

وهي طريقة لإرسال بيانات سرية من خلال تضمينها في وسائط تعد غطاءً حاملاً لها بصورة يتعذر بها تمييز وجود تلك البيانات. وقد تكون الأغطية ملفات نصية أو صورية أو صوتية أو فيديوية، ويمكن أن تكون البيانات السرية نصاً صريحا أو مشفراً أو أية معلومات يمكن تمثيلها على شكل سلسلة من الخلايا الثنائية (Bits). والهدف من الكتابة المغطاة هو نفي الشك بوجود تناقل بيانات سرية[٣].

متطلبات الكتابة المغطاة

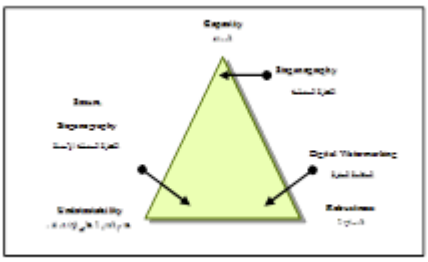
إن المتطلبات التي يجب مراعاتها في تصميم خوارزميات الكتابة المغطاة هي [٤] [الشكل (١)]:

١) السعة Capacity: تشير إلى كمية البيانات التي يمكن تضمينها ضمن غطاء معين.
٢) عدم القدرة على الاكتشاف Undetectability: وتعني عدم قدرة الشخص غير المخول على كشف البيانات المضمنة.
٣) الصلادة Robustness: تشير إلى مدى مقاومة stego-message لهجمات الشخص غير المخول المختلفة قبل تحطيم البيانات المضمنة.

وتعتمد سرية نظام الكتابة المغطاة بالدرجة الأساس على عدم قدرة الشخص غير المخول على التمييز بين الغطاء و-stego message [٥]، ولذلك فإن نجاح النظام يعتمد على سرية الغطاء وعندما يكون الغطاء معلناً فإن نجاح النظام يعتمد على مدى صلادة الخوارزمية المستخدمة. وتتم المحافظة على سرية النظام بجعل الغطاء أكثر صلادة أو باكتشاف أغطية أكثر سرية [٦]. ولأن خوارزميات

* Corresponding author at: University of Mosul - College of Computer Science and Mathematics;

الكتابة المغطاة توفر الاتصال السري من نقطة– إلى– نقطة فهي عادة ليست بحاجة إلى الصلادة أو قد تتمتع بمستوى محدود منها [٤].



الشكل(١): متطلبات الكتابة المغطاة [٤]

تصنيفات الكتابة المغطاة

تصنف الكتابة المغطاة بالاعتماد على المجال الذي تحدث فيه عملية التضمين إلى:

١) **الكتابة المغطاة في المجال المكاني Spatial Domain Steganography**: تقوم على أساس استبدال قيم النقاط الضوئية (Pixel) بالخلايا الثنائية السرية ومن أشهرها خوارزمية استبدال الخلية الثنائية الأقل أهمية (LSB) التي تستبدل قيمة تلك الخلية من كل نقطة بخلية ثنائية من البيانات السرية [٧].

٢) **الكتابة المغطاة في مجال التردد Frequency Domain Steganography**: تُطبِق هنا بعض التحويلات مثل تحويل (DFT) وتحويل (DWT) وتحويل (DCT) على الغطاء لتحويله إلى مجال التردد أولا، ومن ثم تُضَمِن البيانات السرية ضمن المعاملات [٧].

الكتابة المغطاة في مجال الكبس Compression Domain Steganography : ركز في السنوات الأخيرة على تضمين البيانات في مجال الكبس، إذ أن تناقل الملف المكبوس يبعد الشك أكثر مما لو نقل بصورته الأصلية [٨]. ويعد التضمين في ملف مكبوس أكثرَ تعقيداً؛ لان حجم الملف المكبوس يكون اقل من حجم الملف الأصلي مما يجعل التوفيق بين كمية البيانات المضمنة والمحافظة على جودة الصورة مقيداً لدرجة كبيرة. إن معظم الدراسات السابقة تركزت على تضمين البيانات السرية ضمن مجال الكبس المعتمد على خوارزمية التكميم الاتجاهي لفاعليتها في تخفيض حجم الملف مع المحافظة على جودة الصورة نسبياً [١].

دراسات سابقة

قدم Du and Hsu [٧] طريقتين، اعتمدت الأولى على تقسيم الدليل إلى دليلين فرعيين متماثلين وضمنت البيانات في LSB للفهارس بعد أن تم ترتيب الدليل بحسب معدل القيم اللونية. أما الثانية فقد اعتمدت على مبدأ العنقدة (Clustering) لتجميع CW المتشابهة تقريبا في عنقود واحد، وتستمر عملية العنقدة إلى أن يصبح عدد CWs في العنقود الذي ينتمي إليه CW الحالي مساويا للبيانات المراد تضمينها، ويحتاج المستلم إلى الدليل لإعادة عمليات العنقدة من جديد وإرجاع عدد CWs في كل عنقود والذي يمثل البيانات المضمنة [٧].

كما اعتمد Chang and Lin [٨] على تحليل المركبات الرئيسة Principal Component Analysis (PCA) في إعادة ترتيب الدليل وقد ضمّن r من الخلايا الثنائية في الفهارس بطريقة LSB، لكن التضمين لم يحصل على الفهارس كلها؛ لان العملية تعتمد على قيمة حد عتبة معرفة مسبقاً والتي تقارن مع الفرق بين CW الحالي بعد التضمين في فهرسه وبين CWs المشار إليها بالفهارس المجاورة للفهرست الجديد وعليه فإن المستلم يحتاج إلى الدليل وقيمة r وحد العتبة لتحديد الفهرست الذي تم فيه التضمين [٨].

بينما اقترح Chang and Lu [٩] طريقة للتضمين تعتمد على خوارزمية Side-Match Vector Quantization (SMVQ) إذ رُمّزت كتل الصورة التي تقع في الصف الأول والعمود الأول بالطريقة التقليدية ولم تُضمّن أي بيانات سرية فيها، ورُمّزت باقي الكتل بطريقة SMVQ حيث تم تكوين دليل Side Match، ثم قُسم إلى قسمين متماثلين كل قسم مخصص لتضمين قيمة خلية ثنائية 1 أو 0 [٩].

وقد كَوّن Shie [١٠] دليلين: الأول مخصص لترميز (Smooth Area) باستخدام SMVQ مع تضمين البيانات في تلك المناطق، والثاني مخصص لترميز (Complex Area) بالطريقة التقليدية ولم تُستخدم في التضمين. ويحتاج المستلم إلى وجود الدليلين لغرض استخلاص البيانات المضمنة [١٠].

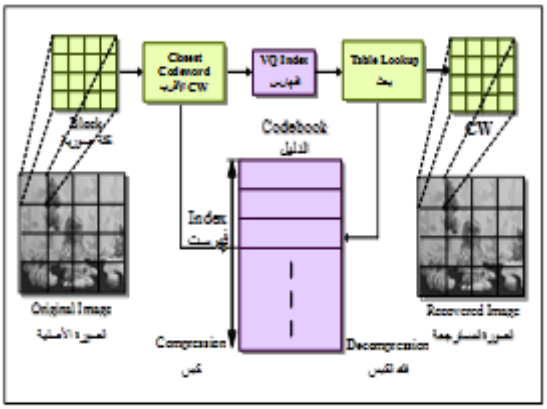
خوارزمية التكميم الاتجاهي

وهي من أكثر الخوارزميات شيوعاً واستخداماً في كبس ملفات الصور إذ ان المبدأ الأساس الذي تقوم عليه هذه الخوارزمية هو استخدام نماذج تقريبية لتمثيل عدد من الكتل المماثلة في الصورة [١١]. يطلق على الكتل الصورية التقريبية Codewords (CW) ويطلق على مجموعة CWs الدليل Codebook (CB) الذي يُكوَّن قبل البدء بعملية الكبس [١٢]. يمكن التعبير عن التكميم الإتجاهي بأنه عملية اقتران Q (Mapping) بين كل متجه من متجهات الصورة x ومتجه واحد من متجهات الدليل C إذ أن: $C = \{y_i, i=1, 2, \ldots, n\}$ ، في حين تمثل كل y_i واحدة من CWs ضمن ذلك الدليل[٧].

$$Q(x) = y_i, x \in R^{k \times k} \quad \ldots\ldots\ldots\ldots\ldots\ldots (1)$$

تُقَسّم الصورة إلى مجموعة من الكتل غير المتداخلة بأبعاد $(k \times k)$ نقطة ضوئية وتمثل بمتجه ذي بعد k^2. ويتحقق الكبس من خلال التعويض عن كل متجه من متجهات الصورة بفهرست من فهارس الدليل بالاعتماد على CW المماثلة له وبذلك تمثَّل الصورة المكبوسة بمجموعة من الفهارس ويطلق عليها جدول الفهارس (Index Table)

[١٢]، أما عملية فك الكبس فهي عملية تعويض عن كل فهرست بقيم CW المقابل له [٧] لاحظ الشكل (٢).



الشكل (٢): عمليتي الكبس و فك الكبس بواسطة خوارزمية التكميم الإتجاهي [١٣]

إن غاية خوارزمية التكميم الاتجاهي هي تقليل التشوه (Distortion) بين متجهات الصورة الأصلية x والمتجهات الناتجة بعد فك الكبس $x^{\wedge}$، ويقصد بالتشوه معدل البعد بين أي متغيرين، ويشار إلى مقدار التشوه بين x و y بـ[d(x,y)] [١٤] ويحسب من القانون الآتي:

$$d(x,y)=\|x-y\|^2=\sum_{l=1}^{k^2}(x_l-y_l)^2 \quad \ldots\ldots(2)$$

حيث ||.|| تمثل المسافة الاقليدية.

إن من أهم القضايا التي تركز عليها خوارزمية التكميم الإتجاهي تكوين دليل جيد، وتعد خوارزمية LBG التي قُدِمت من قبل الباحثين Linde و Buzo و Gray من أكثر طرائق توليد الدليل شيوعاً، وتتضمن تقسيم مجموعة التدريب والبدء بتهيئة دليل ابتدائي ثم تحديثه بصورة تكرارية بإضافة CW جديدة إليه بحيث تحقق أقل تشوه، وفي كل تكرار تقل قيمة هذا التشوه أو تبقى ثابتة كما كانت في التكرار السابق، وتتوقف هذه العمليات عندما تصبح قيمة التشوه أقل من قيمة معرفة مسبقاً [١٤].

الخوارزمية المقترحة:

تتلخص الخوارزمية المقترحة في تضمين خليتين ثنائيتين سريتين في كل فهرست من جدول الفهارس بالاعتماد على باقي قسمة ذلك الفهرست على العدد ٤ وعلى قيمة المفتاح السري، ويتم التضمين من خلال تبديل قيمة الفهرست الحالي بأحد الفهرسين (السابق أو اللاحق) بحيث ينسجم باقي قسمة الفهرست الجديد مع المفتاح السري مع مراعاة اختيار الفهرست الأقرب من بين هذين الفهرسين إلى الفهرست الحالي للمحافظة على جودة الصورة.

خوارزمية التضمين: وتتكون من:

١) **توليد الدليل:** استَخدمت الخوارزمية تقنية التجزئة في توليد الدليل الابتدائي، وأكمَلت توليد الدليل النهائي بتطبيق خوارزمية LBG بعد تحديد بُعد المكمم الاتجاهي (٢×٢) و(٤×٤) وطول دليل ٢٥٦.

٢) **إعادة ترتيب الدليل:** تُرتب الخوارزمية الدليل الناتج بتطبيق تحليل PCAمما يجعل CWs المتقاربة متجاورة مع بعضها البعض، إذ تم إعادة ترتيب CWs تصاعدياً بالاعتماد على قيم نقاط تسقيطها على محور المركب الرئيس الأول،ويعد ترتيب الدليل مهماً جداً لتكوين الصورة الغطاء ولإكمال عملية التضمين بصورة صحيحة وبأقل تشوه.

٣) **الكبس:** تم كبس الصورة بواسطة VQ وباعتماد الدليل المرتب للحصول على الغطاء.

٤) **تهيئة بيانات سرية:** تُقسم البيانات السرية المضمنة إلى قسمين: نص و صورة، وتعتمد الخوارزمية تضمين الكتلة الثنائية (٠) في نهاية البيانات المضمنة للإشارة إلى نهاية البيانات السرية، ويضاف بعدها في حالة تضمين صورة كتلة ثنائية تمثل الطول ثم كتلة ثنائية ثالثة تمثل العرض ليتمكن المستلم من إعادة تشكيل الصورة المسترجعة.

٥) **تضمين البيانات السرية:** اعتمدت الخوارزمية على قانون المسافة الاقليدية بين الفهرست الحالي والفهرسين المجاورين في ايجاد CW الأقرب حيث:

$$I'=\min(dU,dL) \quad \ldots\ldots(3)$$

$$dU=d(I,U)=\sqrt{\sum_{i=l}^{k\times k}(y_{I,i}-y_{U,i})^2} \quad \ldots\ldots(4)$$

$$dL=d(I,L)=\sqrt{\sum_{i=1}^{k\times k}(y_{I,i}-y_{L,i})^2} \quad \ldots\ldots(5)$$

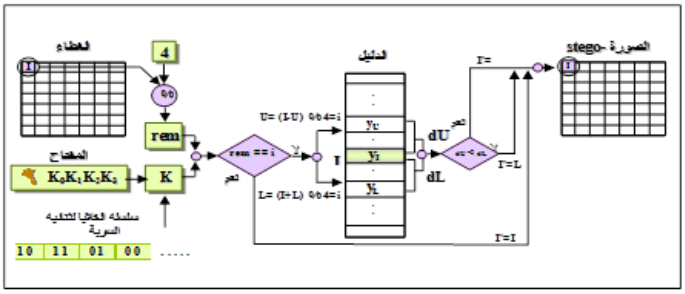
I': تمثل الفهرست الجديد بعد عملية التضمين.

dU: تمثل مقدار المسافة الاقليدية بين الفهرست الحالي (I) والفهرست السابق (U).

dL: تمثل مقدار المسافة الاقليدية بين الفهرست الحالي (I) والفهرست اللاحق (L).

y_I: يمثل CW الحالي.

y_U و y_L: يمثلان CW السابق واللاحق على التوالي.



الشكل (٣): مخطط يوضح خوارزمية التضمين

خصصت الخوارزمية المقترحة خليتين ثنائيتين مختلفتن لكل ناتج من نواتج باقي القسمة حسب قيمة المفتاح السري الذي يتكون من أربعة أرقام هي (0,1,2,3) مرتبة بصورة عشوائية (على سبيل المثال 1032) وخوارزمية التضمين موضحة في الشكل(٣).

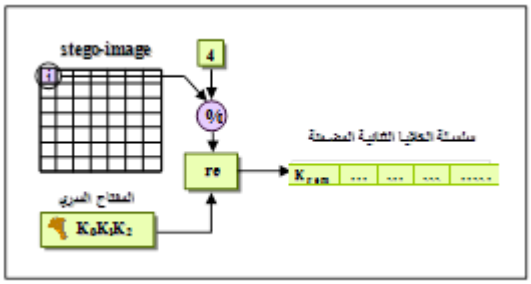
إن باقي قسمة الأعداد على ٤ تنحصر ضمن الفترة (0,3)؛ لذلك فإن البيانات المضمنة قد تكون 00 أو 01 أو 10 أو 11. كما ان استخدام المفتاح $Key=K_0K_1K_2K_3$ الذي يتكون من أربعة أرقام (0,1,2,3) مرتبة بصورة عشوائية (مثلاً 1032 أو 3210 أو حسب الاتفاق بين الطرفين) أضاف مستوى آخر للسرية إذ تعمد الخوارزمية في حالة كون البيانات هي K_i إلى تبديل الفهرست الحالي بأحد الفهرسين المجاورين له بحيث يصبح باقي قسمة الفهرست المستبدل على ٤ مساويا ل(i)، الجدول(١).

جدول (١): تطبيق التضمين على الفهارس بالاعتماد على باقي القسمة على ٤ وعلى المفتاح السري

قيمة الخليتين الثنائيتين السريتين	باقي قسمة الفهرست الحالي (I) على ٤	قيمة الفهرست السابق	قيمة الفهرست اللاحق	قيمة الفهرست الجديدة (I')
K_0	٠	--	--	I
	١	I – 1	I + 3	I': فهرست CW الأقرب
	٢	I – 2	I + 2	
	٣	I – 3	I + 1	
K_1	٠	I – 3	I + 1	I': فهرست
	١	--	--	I
	٢	I – 1	I + 3	I': فهرست CW الأقرب
	٣	I – 2	I + 2	
K_2	٠	I – 2	I + 2	I': فهرست CW الأقرب
	١	I – 3	I + 1	
	٢	--	--	I
	٣	I – 1	I + 3	I': فهرست
K_3	٠	I – 1	I + 3	I': فهرست CW الأقرب
	١	I – 2	I + 2	
	٢	I – 3	I + 1	
	٣	--	--	I

خوارزمية الاستخلاص

يقوم المستلم باستخلاص البيانات السرية بالاعتماد على قيمة المفتاح السري نفسه، ولا يحتاج لوجود الدليل لغرض استخلاص البيانات إذ يحسب المستلم باقي قسمة الفهارس على ٤ ويطابق الناتج مع المفتاح السري ليحصل على القيمة المضمنة بصورتها الصحيحة، فإذا كان باقي قسمة فهرست معين يساوي i فإن القيمة المضمنة فيه هي K_i وكما مبين في الشكل (٤).



الشكل (٤): مخطط يوضح خوارزمية الاستخلاص

٨- قياس كفاءة الخوارزمية

قيست كفاءة الخوارزمية المقترحة باعتماد المعايير الرئيسة لتقييم كفاءة خوارزميات الكتابة المغطاة ضمن مجال الكبس المعتمد على خوارزمية التكميم الاتجاهي وكالآتي[١٢]:

١) **مقياس PSNR**: تم حسابه بين (الغطاء وstego-image) للتأكد من جودة الصورة الناتجة.

٢) **نسبة الكبس Compression Ratio**: وتحسب من خلال القانون الآتي:

$$CR = \frac{number\ of\ bits\ in\ compressed\ stream}{number\ of\ pixels\ in\ VQ\ image}(bpp)\ ....(6)$$

٣) **سعة التضمين Embedding Capacity (EC)**: ويقصد بها الحد الأعلى لعدد الخلايا الثنائية التي يمكن أن تُضَمّن ضمن جدول الفهارس [١]. وتحسب من خلال المعادلة الآتية:

$$nBits = (H' \times W' \times 2) - x\ bits.....(7)$$

H',W' أبعاد الصورة الغطاء، و x الكتلة الثنائية الإضافية (حالة النص=٨) (حالة الصورة=٤).

٤) **كفاءة التضمين Embedding Efficiency (EE)**: وتحسب من خلال المعادلة الآتية:

$$EE = \frac{number\ of\ secret\ bits}{number\ of\ bits\ in\ a\ compressed\ stream}.....(8)$$

عرض النتائج ومناقشتها

أجريت اختبارات متعددة للخوارزمية المقترحة على صور JPG مختلفة الأبعاد رمادية وملونة، مع تضمين نص وصورة كل على حدة مع قيم مختلفة من المفتاح السري، الجدول (٢):

جدول (٢): نتائج تضمين نص في صور JPG رمادية

الصورة الأصلية	الأبعاد (Pixel)	بُعد المكعم الاتجاهي (Pixel)	سعة التضمين القصوى (Bit)	PSNR in dB stego/الغطاء (بعد الكبس)	BER %
Ship.JPG	٦٠٠×٥٠٠	٤	٣٤٢٨١	٤١.٦٠٠٦	٠
		٢	١٢٩٩٨٢	٤١.٣٢٢٣	٠
Fish.JPG	٥١٢×٥١٢	٤	٣١٥٣٣	٤٣.٥٥١١	٠

		٢	١١٨٨٤٢	٤٣.٥٠٠١	٠
Tiger.JPG	512×512	٤	٣١٥٣٣	٤٠.٤١١٢	٠
		٢	١١٨٨٤٢	٤١.٠٠١٥	٠

إن تقليل بُعد المكمم الاتجاهي من ٤ إلى ٢ يؤدي إلى زيادة سعة التضمين القصوى بمقدار أربعة أضعاف تقريبا والسبب هو ازدياد عدد الفهارس، كما تزداد جودة الصورة المسترجعة حسب قيم PSNR.

ومن خلال ملاحظة قيم PSNR يتبيّن أن الخوارزمية المقترحة قد ضَمّنت الحد الأعلى لطول النص في الغطاء من دون حدوث تشوهات ملحوظة؛ وذلك لأن التضمين في الفهارس اعتمد على تبديل الفهرست الحالي بناءً على التشابه بينه وبين الفهارس المجاورة له في الدليل. اما استخلاص البيانات المضمنة فقد كان كاملاً من دون أخطاء، حسب قيم Bit Error Rate (BER). لاحظ الجدول(٣).

استطاعت الخوارزمية تضمين صور رمادية بأبعاد جيدة تعتمد على بُعد المكمم الاتجاهي وعلى أبعاد الصورة الأصلية. وأن قيمة BER تُبين أن استخلاص الصور المضمنة كان دون أخطاء.

جدول (٣): نتائج تضمين صورة رمادية في صور JPG رمادية

الصورة الأصلية	الأبعاد Pixel	بُعد المكمم الاتجاهي (Pixel)	الصورة السرية	أبعاد الصورة السرية (Pixel)	PSNR in dB الغطاء/ Stego (بعد الكبس)	BER%
Boat .JPG	×٤٦٠ ٦٠٠	٤	Chess	54×54	٤٠.٠٠٦١	٠
		٢	Girl	99×118	٤١.٠٠٠١	٠
Phone .JPG	512× 400	٤	mandr	55×55	41.7211	٠
		٢	Boats	110×110	41.4188	٠
TV.JPG	512× 512	٤	bird	66×62	٤٠.٩١٠١	٠
		٢	moon	128×127	٤١.٦٩١١	٠

طُبقت الخوارزمية على صور ملونة وكونت دليلا منفصلا لكل مستوى لوني ثم طبقت خوارزمية الكبس على كل مستوى لوني من RGB كل على حدة، ثم دمجت سويةً مع بعضها للحصول على صورة الغطاء. كما طبقت خوارزمية التضمين على مستوى لوني واحد وهو الأحمر إذ كان الافضل نسبياً من المستويين الآخرين فيما يتعلق بقيمتي BER و PSNR. لاحظ الجدول (٤).

جدول (٤): نتائج تضمين نص في صور JPG ملونة

الصورة الأصلية	الأبعاد (Pixel)	بُعد المكمم الاتجاهي (Pixel)	سعة التضمين القصوى (Bit)	PSNR in dB الغطاء stego/ (بعد الكبس)	BER %
Mirror .JPG	256×256	٤	7879	52.1176	0.3
		٢	٣١٥٠١	51.0018	0.9
Book .JPG	600×400	٤	23809	52.0011	0.1
		٢	100012	51.0233	0.9
Linux .JPG	256×256	٤	7879	51.0010	0.6
		٢	٣١٥٠١	50.7161	0.5

تم احتساب قيمة PSNR من خلال إيجاد معدل قيمها للمستويات اللونية الثلاثة فكانت قيمتها تساوي Inf لأن عملية التضمين استخدمت المستوى اللوني الأحمر فقط، ولغرض إثبات تلك القيمة تم احتسابها بعد التحويل إلى النظام اللوني YCbCr واعتماد المستوى Y فقط، فكانت النتائج كما هو مبين في الجدول ضمن الحقل نفسه. وتشير قيم BER إلى أن هناك نسبة فقدان ضئيلة جدا للمعلومات المضمنة في الصور الملونة نتيجة تأثرها بالكبس، إلا أن هذه النسبة كانت غير ملحوظة إذا ما قورنت بطول النص المضمن. أما نتائج تضمين صور رمادية في صور ملونة فكما هو مبين في الجدول (٥).

جدول (٥): نتائج تضمين صور رمادية في صور JPG ملونة

الصورة الأصلية	الأبعاد Pixel	بُعد المكم الاتجاهي (Pixel)	الصورة السرية	أبعاد الصورة السرية (Pixel)	PSNR in dB الغطاء/stego (بعد الكبس)	BER %
Fruit .JPG	256 ×256	4	Key	30×34	51.0231	0.3
		٢	Boy	48×50	52.4110	0.4
Garden .JPG	٤٠٠ ×٥٠٠	٤	Bird	45×45	50.1912	0.3
		٢	Moon	91×91	51.0012	0.4
Sky .JPG	256 ×256	٤	Key	30×34	51.6540	0.2
		٢	cartoon	64×63	51.5321	0.2

بلغت نسبة كبس أي صورة في الخوارزمية المقترحة (2 bpp) إذا كان بُعد المكمم الاتجاهي ٢×٢، وتزداد نسبة الكبس إلى (0.5 bpp) عندما يزداد بُعد المكمم الاتجاهي إلى ٤×٤. كما بلغت كفاءة تضمين الخوارزمية المقترحة 0.23 والمحسوبة من المعادلة (٨). وقد أجريت التجارب باستخدام حاسوب نوع Pentium4 بمواصفات (CPU 1.60 GHz =، RAM =1 GB). ولابد من الإشارة إلى أن الزمن المستغرق في التضمين تضمّن زمن توليد دليل الصورة الذي يزداد بازدياد الأبعاد وتقليل بُعد المكمم الاتجاهي. كما أن زمن التضمين في الصور الملونة كان أعلى منه في الصور الرمادية نتيجة لزيادة الوقت المستغرق في توليد دليل الصور الملونة.

الاستنتاجات

يمكن المحافظة على جودة الصورة من خلال إضافة شروط مقيدة لاختيار CWs مناسبة أثناء عملية التضمين. كما إن استخدام الدليل المحلي، بوصفه الدليل المثالي لكبس الصورة، للحصول على الغطاء أعطى تنوعا للأغطية المستخدمة في التضمين أكثر من الدليل العام لاسيما وأن الكتابة المغطاة تتطلب إرسال صور مختلفة عن الصور السابقة في كل اتصال. وكان لبُعد المكمم الاتجاهي تأثيراً كبيراً على جودة الصورة وكمية البيانات المضمنة. كما إن استخلاص البيانات المضمنة دون الحاجة لوجود الدليل كان لها الأثر الكبير في تقليل الزمن المستغرق في العملية. اما الصور الملونة فإن تطبيق

التضمين على مستوى لوني واحد يحافظ كثيراً على جودة الصورة لأنه لن يؤثر الا على المستوى اللوني ذاته.

المصادر

[1] Wang Z. H., Chen K. N., Chang C. C., and Li M. C., (2009). "Hiding Information in VQ Index Tables with Reversibility". Proceedings of the International Symposium on Intelligent Information Systems and Applications, China.

[2] Motameni H., Norouzi M., Jahandar M., and Hatami A., (2007). "Labeling Method in Steganography". *World Acad. Sci. Eng. Technol*., Issue 30, pp. 349-354.

[3] Amin F., Soleimanipour M., and Karimi A., (2008). "A Novel Plausible Deniability Scheme in Secure Steganography". *World Academy of Science, Engineering and Technology*, Vol. 43, pp.217-219.

[4] Hovancak R., Foris P., & Levicky D., (2006). "Steganography Based on DWT Transform". *In: Radioelektronika 16th international Czech - Slovak scientific conference*: Conference Proceedings. Bratislava. Slovak University of Technology, Czech.

[5] Katzenbeisser S. C., and Petitcolas F. A. P., (2000). "Information hiding techniques for steganography and Digital Watermarking". *Artech House*, Bosten, London.

[6] Potdar V., and Chang E., (2004). "Visibly Invisible: Ciphertext as a Steganographic Carrier". *4th International Network Conference*, Plymouth U.K.

[7] Du W. C. and Hsu W. J., (2003). "Adaptive Data Hiding Based on VQ Compressed Images". *IEEE Proc.-Vis. Image Signal Process*., Vol. 150, No. 4, pp. 233-238.

[8] Chang C.C., & Lin P.Y., (2004). "A Compression-Based Data Hiding Scheme Using Vector Quantization and Principal Component Analysis". *International Conference on Cyberworlds*, Tokyo, Japan.

[9] Chang C. C., and Lu T. C., (2006). "Reversible Index-Domain Information Hiding Scheme Based on Side-Match Vector Quantization". *The Journal of Systems and Software*, Vol. 79, Issue 8. pp.1120–1129.

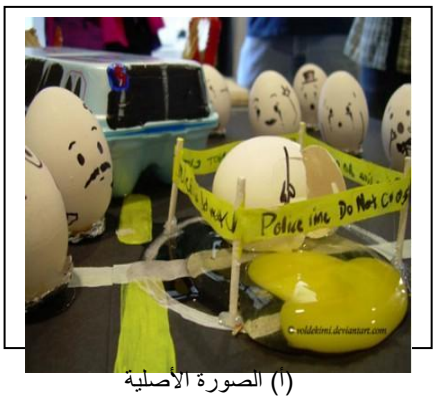
[10] Shie C. S., Lin S. D., and Fang C. M.,(2006)."Adaptive Data Hiding Based on SMVQ Prediction". *IEICE Trans. Inf. & Syst*., Vol. 89, No.1, pp.358-362.

[11] Lin C. C., Chen S. C., and Hsueh N. L.,(2009). "Adaptive Embedding Techniques for VQ-Compressed Images". *Information Sciences*, Vol. 179, Issues 1-2, pp.140–149 .

[12] Chang C. C., Lin P. Y., and Wang H. C., (2009). "Distortion-Free Steganography Mechanism with Compression to VQ Indices". *International Journal of Signal Processing, Image Processing and Pattern Recognition*, Vol. 2, No. 2, pp. 39-52.

[13] Lin C. Y., and Chang C. C., (2006). "Hiding Data in VQ-Compressed Images Using Dissimilar Pairs". *Journal of Computers*, Vol.17, No.2, pp.3-10.

[14] Saffar H. E., (2008). "Channel Optimized VQ: Iterative Design Algorithms". *MSc Thesis, Dept of Mathematics & Statistics, Queen's University*, Kingston, Canada.



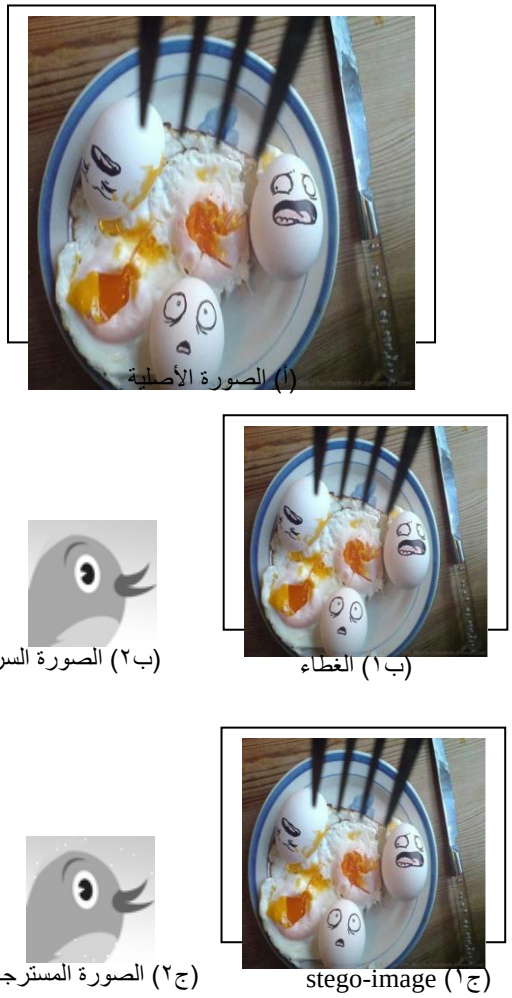
(أ) الصورة الأصلية

(ب) الغطاء

stego-image (ج)

شكل (5): تضمين نص في صورة JPG
رمادية بُعد المكمم =٤

P- ISSN 1991-8941 , E-ISSN 2706-6703 (*JUAPS*) مجلة جامعة الانبار للعلوم الصرفة Open Access
2012 ,(6), (2) :13-19



شكل (6): تضمين صورة رمادية في صورة JPG
ملونة بُعد المكمم =٢

A New VQ Technique for Steganography in JPG

Ahmed Sami Nori **Ansam Osama Abdulmajeed**

Abstract:

The present research was aimed to implement a new Steganographic algorithm for colored images in Vector Quantization (VQ) compressed domain, since the compressed image considers a secure cover for data to be embedded to avoid attention of unauthorized persons. Also, it saves the cost and time of transmission and storage. The new algorithm aimed to increase the embedding capacity with maintaining the image quality as well as reducing the time of the extraction process. The algorithm was implemented using Matlab 2009a. It embedded two bits in each index depending on mod 4, and secret key shared between sender and receiver. The algorithm used grayscale and RGB images for (JPG) of different resolutions after compression in order to be used as a cover of secret data which were either as text or image. In the research, the new algorithm provided an acceptable image quality despite of the high embedding capacity that occupy the cover image completely, Also, the codebook was not needed for data extraction which led to reducing the extraction time significantly.