Steganography based on Vector Quantization Technique

Ansam Osamah

Ahmed S. Nori

ansam_osamah@uomosul.edu.iq

ahmed.s.nori@uomosul.edu.iq

College of Computer Science and Mathematics

University of Mosul, Mosul, Iraq

Received on: 29/09/2011

Accepted on: 14/12/2011

ABSTRACT

The present research was aimed to implement a new Steganographic algorithm for 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 (BMP and PNG) 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.

Keywords: Steganography, VQ, BMP, PNG, codebook.

الكتابة المغطاة بالاعتماد على تقنية التكميم الاتجاهي

أنسام أسامة عبد المجيد

أحمد سامي نوري

كلية علوم الحاسوب والرياضيات

جامعة الموصل، الموصل، العراق

تاريخ قبول البحث: 2011/12/14

تاريخ استلام البحث: 2011/09/29

الملخص

يهدف البحث الحالي إلى تصميم وتنفيذ خوارزمية جديدة للكتابة المغطاة في الصور ضمن مجال الكبس باستخدام خوارزمية التكميم الاتجاهي (VQ) Vector Quantization، كون الملف المكبوس يعد غطاءً آمناً للبيانات المضمنة ويُجنّب إثارة انتباه الأشخاص غير المخولين، ويوفر كلاً من كلفة وزمن النقل والخرن. وتهدف الخوارزمية إلى زيادة كمية سعة التضمين مع المحافظة على جودة الصورة، فضلاً عن تقليل زمن عملية الاستخلاص. نُقِّدَت الخوارزمية المقترحة باستخدام Matlab 2009a، واعتمدت في تضمين البيانات في كل فهرس على باقي قسمته على 4 وعلى مفتاح سري مشترك بين الطرفين، كما استُخدمت صوراً رمادية وملونة بأبعاد مختلفة وبامتدادي (BMP) و (PNG). بعد كبسها لتكون غطاءً للبيانات السرية التي كانت نصاً أو صورة. تبين من البحث أن الخوارزمية المقترحة قد حافظت على جودة مقبولة 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.

الكلمات المفتاحية: الكتابة المغطاة، التكميم الاتجاهي، BMP، PNG، دليل الصور.

1- المقدمة

نتيجة التطور الكبير في تقنيات الشبكات أصبح بإمكان الكثيرين الاتصال مع بعضهم البعض بسهولة وبسرعة عبر الإنترنت. ولأن الإنترنت بيئة عامة ومفتوحة فبإمكان أي شخص غير مخول مراقبة معلومات متناقلة بين أي طرفين واعتراضها أو الحصول عليها؛ لذا فإن أهمية توفير الأمانة لتلك المعلومات تتزايد يوماً بعد يوم للحفاظ على سريتها [17].

هناك تقنيتان لتوفير الأمانة للمعلومات المتناقلة وهما التشفير (Encryption) والكتابة المغطاة (Steganography)، 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 لاستخدام الكتابة المغطاة؛ إذ أنها تقنية تُضمّن بيانات سرية داخل بيانات أخرى بحيث لا يمكن ملاحظتها مما يخفي حقيقة البيانات السرية المتناقلة [13].

2- الكتابة المغطاة

الكتابة المغطاة هي 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 صوتية أو فيديو، ويمكن أن تكون البيانات السرية نصاً صريحاً 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 [1].

3- متطلبات الكتابة المغطاة

إن المتطلبات التي يجب مراعاتها في تصميم خوارزميات الكتابة المغطاة هي [9] [الشكل (1)]:

- (1) السعة Capacity: تشير إلى كمية البيانات التي يمكن تضمينها ضمن غطاء معين.
- (2) عدم القدرة على الاكتشاف Undetectability: عدم قدرة الشخص غير المخول على كشف البيانات.
- (3) الصلابة 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 [10]، ولذلك فإن نجاح النظام يعتمد على سرية الغطاء وعندما يكون الغطاء معلناً فإن نجاح النظام يعتمد على مدى صلابة الخوارزمية المستخدمة. وتتم المحافظة على سرية النظام بجعل الغطاء أكثر صلابة أو باكتشاف أغطية أكثر سرية [14]. ولأن خوارزميات الكتابة المغطاة تتعلق بتوفير الاتصال السري من نقطة - إلى - نقطة فهي عادة ليست بحاجة إلى الصلابة أو قد تتمتع بمستوى محدود منها [9].

الشكل (1): متطلبات الكتابة المغطاة [9]

4- تصنيفات الكتابة المغطاة

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

- (1) **الكتابة المغطاة في المجال المكاني Spatial Domain Steganography**: تقوم على أساس استبدال قيم النقاط الضوئية (Pixel) بالخلايا الثنائية السرية ومن أشهر خوارزمياتها خوارزمية استبدال الخلية الثنائية الأقل أهمية (LSB) التي تستبدل قيمة تلك الخلية من كل نقطة بخلية ثنائية من البيانات السرية [8].
- (2) **الكتابة المغطاة في مجال التردد Frequency Domain Steganography**: تُطبق هذه طرائق بعض التحويلات مثل تحويل (DFT) وتحويل (DWT) وتحويل (DCT) على الغطاء لتحويله إلى مجال التردد أولاً، ومن ثم تُضمّن البيانات السرية ضمن المعاملات [8].
- (3) **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 [7]. ويعد التضمين في ملف مكبوس أكثر تعقيداً؛ لأن حجم الملف المكبوس يكون أقل من حجم الملف الأصلي مما يجعل التوفيق بين كمية البيانات المضمنة والمحافظة على جودة الصورة مقيداً لدرجة كبيرة [25، 26]. إن معظم الدراسات السابقة تركّزت على تضمين البيانات السرية ضمن مجال الكبس المعتمد على خوارزمية التكميم الاتجاهي لفاعليتها في تخفيض حجم الملف مع المحافظة على جودة الصورة نسبياً [17] إذ تتدرج طرائق الكتابة المغطاة ضمن هذا المجال تحت صنفين الأول: طرائق التضمين الثابتة (Fixed Embedding Methods) التي تعتمد على تقسيم الدليل إلى دليلين فرعيين والانتقال من دليل إلى آخر بحسب قيمة الخلية الثنائية السرية أو تُضمّن البيانات بطريقة LSB ضمن الفهارس، إلا أن كمية البيانات تكون ثابتة، فضلاً عن حصول نسبة من التشوه في الصورة بسبب الانتقال من دليل فرعي إلى آخر [8]. كما أن زيادة كمية البيانات سوف تكون على حساب المحافظة على جودة الصورة [12]. والثاني طرائق التضمين التكيفية (Adaptive Embedding Methods) التي تستند على إعادة تجميع (Codeword CW) ضمن عناقيد حسب قيمة البيانات السرية [8] أو تخصيص قيمة لكل CW ضمن العنقود نفسه وتزداد كمية البيانات في كل فهرست أو تقل حسب قيمة عتبة معينة [11]، لكن هذه الطرائق بحاجة إلى إعادة تجميع وترتيب CW في كل مرة لكي تتلاءم مع البيانات مما يستغرق وقتاً طويلاً، ويجب إعادة عمليات التجميع نفسها للحصول على البيانات بصورة صحيحة [16].

وقد صنفت طرائق الكتابة المغطاة في هذا المجال بالاعتماد على مبدأ المعكوسية وهو إمكانية إرجاع الصورة (stego-image)، بعد استخلاص البيانات، إلى أصلها قبل التضمين إلى:

- طرائق التضمين غير القابلة للعكس (Irreversible Embedding Methods).
- طرائق التضمين القابلة للعكس (Reversible Embedding Methods).
- طرائق التضمين شبه القابلة للعكس (Nearly Reversible Embedding Methods) [6].

5- دراسات سابقة

قدم Du and Hsu [8] 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 [8].

كما اعتمد Chang and Lin [7] على تحليل المركبات الرئيسية Principal Component Analysis (PCA) في إعادة ترتيب الدليل وقد ضَمَّن r من الخلايا الثنائية في الفهارس بطريقة LSB، لكن التضمين لم يحصل على الفهارس كلها؛ لأن 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 [7].

بينما اقترح Chang and Lu [4] طريقة للتضمين تعتمد على خوارزمية Side-Match Vector Quantization (SMVQ) إذ رُمِزَت كتل الصورة التي تقع في الصف الأول والعمود الأول بالطريقة التقليدية ولم تُضَمَّن أي بيانات سرية فيها، ورُمِزَت باقي الكتل بطريقة SMVQ حيث تم تكوين دليل Side Match، ثم قُسم إلى قسمين متماثلين كل قسم مخصص لتضمين قيمة خلية ثنائية إما 1 أو 0 [4].

وقد كَوَّن Shie [16] 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 [16].

6- 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 [11]. يطلق على الكتل الصورية التقريبية (CW) Codewords ويطلق على مجموعة CWs الدليل (CB) Codebook الذي يُكوَّن قبل البدء بعملية الكبس [6]. يمكن التعبير عن التكميم الاتجاهي بأنه عملية اقتران Q (Mapping) بين كل متجه من متجهات الصورة x ومتجه واحد من متجهات الدليل C إذ أن $C = \{y_i, i=1, 2, \dots, n\}$ ، في حين تمثل كل واحدة من CWs ضمن ذلك الدليل [8].

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

تُقسَّم 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 تمثل الصورة المكبوسة بمجموعة من الفهارس ويطلق عليها جدول الفهارس (Index

(Table [6])، أما عملية فك الكبس فهي عملية تعويض عن كل فهرست بقيم CW المقابل له [8] لاحظ الشكل (2).

الشكل (2): عمليتي الكبس و فك الكبس بواسطة خوارزمية التكميم الاتجاهي [12]

إن غاية خوارزمية التكميم الاتجاهي هي تقليل التشوه (Distortion) بين متجهات الصورة الأصلية x والمتجهات الناتجة بعد فك الكبس x^h ، ويقصد بالتشوه معدل البعد بين أي متغيرين، ويشار إلى مقدار التشوه بين x و y بـ $d(x,y)$ [15] ويحسب من خلال القانون الآتي:

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

حيث $\|\cdot\|$ تمثل المسافة الاقليدية.

إن من أهم القضايا التي تركز عليها خوارزمية التكميم الاتجاهي تكوين دليل جيد، وتعد خوارزمية LBG التي قُدمت 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 [15].

7- تحليل المركبات الرئيسية

يعد تحليل المركبات الرئيسية من التحليلات التي تستخدم في ترتيب المتجهات متعددة الابعاد، وتتحقق إعادة ترتيب تلك المتجهات من خلال ترتيب نقاط التسقيط المقابلة لها [5]. ويعد محور المركب الرئيسي الأول أكثر المحاور الذي يُبقي على أكثر الاختلافات بين المتجهات الأصلية، لذلك يمكن ترتيب المتجهات بالاعتماد على قيم نقاط تسقيطها عليه [3]. وتحسب المركبات الرئيسية من خلال القيم الذاتية (Eigenvalues) والمتجهات الذاتية (Eigenvector) لمصفوفة التغاير (Covariance Matrix) التي تحسب من خلال القانون الآتي:

$$Cov(X, Y) = \sum_{i=1}^N \frac{(x_i - \bar{x})(y_i - \bar{y})}{N} \quad \dots(3)$$

حيث أن N تمثل عدد الأبعاد بينما تمثل $\bar{x}$ و $\bar{y}$ معدل البعدين X و Y على التوالي. ويمكن إيجاد القيم الذاتية (λ) والمتجهات الذاتية المقابلة لها (X) من مصفوفة التباين (A) تحت الشرط $AX = \lambda X$ ، من خلال ما يأتي [2]:

(1) إيجاد القيم الذاتية λ من خلال حل المعادلة الآتية:

$$|A - \lambda I| = 0 \quad \dots(4)$$

I : تمثل المصفوفة الأحادية (Identity Matrix) بأبعاد المصفوفة A نفسها.

$| \cdot |$: يمثل محدد المصفوفة.

وتستخدم المعادلة (4) في إيجاد المعادلة المميزة (Characteristic Equation) لمصفوفة التباين (A) ومن ثم إيجاد القيم الذاتية (λ)، فإذا كانت أبعاد المصفوفة (A) هي $N \times N$ فإن القيم الذاتية الناتجة هي $\lambda_1, \lambda_2, \dots, \lambda_N$. ثم يعاد ترتيبها بحيث $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_N$.

(2) إيجاد المتجهات الذاتية $X_1, X_2, \dots, X_N$ المقابلة لكل قيمة ذاتية من خلال حل المعادلة الآتية:

$$(A - \lambda I) X = 0 \quad \dots(5)$$

حيث تمثل X_i اتجاه المركب الرئيس i ، ويمتلك X_1 أعلى قيمة ذاتية (أي أعلى تباين).

8- الخوارزمية المقترحة:

تتلخص الخوارزمية المقترحة في تضمين خليتين ثنائيتين سريتين في كل فهرست من جدول الفهارس بالاعتماد على باقي قسمة ذلك الفهرست على العدد 4 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.

8-1 خوارزمية التضمين: تتكون خوارزمية التضمين من خمس مراحل رئيسية هي:

- (1) **توليد الدليل:** استُخدمت الخوارزمية تقنية التجزئة في توليد الدليل الابتدائي، وأُكملت توليد الدليل النهائي بتطبيق خوارزمية LBG بعد تحديد بُعد المكعب الاتجاهي (2×2) و (4×4) وطول دليل 256.
- (2) **إعادة ترتيب الدليل:** تُرتب الخوارزمية الدليل الناتج بتطبيق تحليل PCA مما 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 وإكمال عملية التضمين بصورة صحيحة وبأقل تشوه.

(3) **الكبس:** تم كبس الصورة بواسطة VQ وبعتماد الدليل المرتب للحصول على الغطاء.

- (4) **تهيئة بيانات سرية:** تُقسم البيانات السرية المضمنة إلى قسمين: نص و صورة، وتعتمد الخوارزمية تضمين الكتلة الثنائية (0) في نهاية البيانات السرية للإشارة إلى نهاية البيانات السرية، ويضاف بعدها في حالة تضمين صورة كتلة ثنائية تمثل طول الصورة ثم كتلة ثنائية ثالثة تمثل عرض الصورة ليتمكن المستلم من إعادة تشكيل الصورة المسترجعة.

(5) **تضمين البيانات السرية:** اعتمدت الخوارزمية على قانون المسافة الاقليدية بين الفهرست الحالي والفهرسين المجاورين في إيجاد CW الأقرب وكما يأتي:

$$I' = \min (dU, dL) \quad \dots(6)$$

$$dU = d(I, U) = \sqrt{\sum_{i=1}^{k \times k} (y_{I,i} - y_{U,i})^2} \quad \dots(7)$$

$$dL = d(I, L) = \sqrt{\sum_{i=1}^{k \times k} (y_{I,i} - y_{L,i})^2} \quad \dots(8)$$

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_L و y_U : يمثلان CW السابق واللاحق على التوالي.

خصصت الخوارزمية المقترحة خليتين ثنائيتين مختلفتين 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 هذه موضحة في الشكل (3).

الشكل (3): مخطط يوضح خوارزمية التضمين

إن باقي قسمة الأعداد على 4 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 (على سبيل المثال 1032 أو 3210 أو حسب الاتفاق بين الطرفين) أضاف مستوى آخر للسرية إذ تعتمد الخوارزمية في حالة كون البيانات هي K_i إلى تبديل الفهرست الحالي بأحد الفهرسين المجاورين له بحيث يصبح باقي قسمة الفهرست المستبدل على 4 مساويا لقيمة i وكما في الجدول (1).

8-2- 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 4 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 (4).

الشكل (4): مخطط يوضح خوارزمية الاستخلاص

جدول (1): تطبيق التضمين على الفهارس بالاعتماد على باقي القسمة على 4 وعلى المفتاح السري

قيمة الخليتين الثنائيتين السريتين	باقي قسمة الفهرست الحالي (I) على 4	قيمة الفهرست السابق	قيمة الفهرست اللاحق	قيمة الفهرست الجديدة (I')
K ₀	0	--	--	I
	1	I - 1	I + 3	I: فهرست CW الأقرب
	2	I - 2	I + 2	
	3	I - 3	I + 1	
K ₁	0	I - 3	I + 1	I: فهرست CW الأقرب
	1	--	--	I
	2	I - 1	I + 3	I: فهرست CW الأقرب
	3	I - 2	I + 2	
K ₂	0	I - 2	I + 2	I: فهرست CW الأقرب
	1	I - 3	I + 1	
	2	--	--	I
	3	I - 1	I + 3	I: فهرست CW الأقرب
K ₃	0	I - 1	I + 3	I: فهرست CW الأقرب
	1	I - 2	I + 2	
	2	I - 3	I + 1	
	3	--	--	I

9- قياس كفاءة الخوارزمية

قيست كفاءة الخوارزمية المقترحة باعتماد المعايير الرئيسة لتقييم كفاءة خوارزميات الكتابة المغطاة ضمن مجال الكبس المعتمد على خوارزمية التكميم الاتجاهي وكالاتي [6]:

(1) مقياس PSNR: تم حسابه في حالة الكبس بين الغطاء و stego-image للتأكد من أن جودة الصورة الناتجة جيدة بحيث يتعذر تمييزها بصريا عن الغطاء، ثم حسابه للصورة بعد فك الكبس، بين كل من الصورة الأصلية والغطاء والصورة الأصلية و stego-image لمعرفة مدى معكوسية الخوارزمية.

(2) نسبة الكبس Compression Ratio: وتحسب من خلال القانون الآتي:

$$CR = \frac{\text{number of bits in compressed stream}}{\text{number of pixels in VQ image}} (bpp) \quad \dots (9)$$

3) سعة التضمين (Embedding Capacity (EC): ويقصد بها الحد الأعلى لعدد الخلايا الثنائية التي يمكن أن تُضمّن ضمن جدول الفهارس [17]. ويمكن حساب السعة القصوى للتضمين في الخوارزمية المقترحة من خلال المعادلة الآتية:

$$nBits = (H' \times W' \times 2) - x \text{ bits} \quad \dots(10)$$

H', W' يمثلان أبعاد الصورة المغطاة، و x الكتلة الثنائية الإضافية، وقيمتها $=8$ في حالة النص و $=24$ في حالة الصورة.

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

$$EE = \frac{\text{number of secret bits}}{\text{number of bits in a compressed stream}} \quad \dots(11)$$

10- عرض النتائج ومناقشتها

أجريت اختبارات متعددة للخوارزمية المقترحة على صور مختلفة الأبعاد رمادية وملونة وبلاامتدادين BMP و PNG، واعتمدت تضمين نص وصورة كل على حدة وباستخدام قيم مختلفة من المفتاح السري، وكانت النتائج كما مبين في الجدول (2):

جدول (2): نتائج تضمين نص في صور رمادية

BER	PSNR in dB		طول النص السري (Bit)	سعة التضمين القصوى (Bit)	PSNR in dB الأصل/الغطاء	بُعد المكمم الاتجاهي (Pixel)	الأبعاد (Pixel)	الصورة الأصلية
	بعد فك الكبس	بعد الكبس						
	stego/الأصل	stego/الغطاء						
0	24.4354	42.6128	35392	35392	30.9672	4	472×600	Horse.bmp
0	29.0669	42.4683	141592	141592	35.4749	2		
0	31.741	45.868	16384	327 60	35.9548	4	512×512	Child.bmp
0	36.8867	45.8905	65536	131064	39.8165	2		
0	27.9834	42.5276	32760	327 60	35.4939	4	512×512	Clock.png
0	33.4434	42.7506	131064	131064	39.9858	2		

إن تقليل بُعد المكمم الاتجاهي من 4 إلى 2 يؤدي إلى زيادة سعة التضمين القصوى بمقدار أربعة أضعاف تقريباً والسبب هو ازدياد عدد الفهارس، كما تزداد جودة الصورة المسترجعة حسب قيم PSNR.

ومن خلال ملاحظة قيم PSNR بين الصورة المغطاة والصورة stego-image بعد الكبس يتبين أن الخوارزمية المقترحة ضمنت الحد الأعلى لطول النص في الغطاء من دون أن تحدث تشوهات ملحوظة؛ وذلك لأن عملية التضمين في الفهارس اعتمدت على تبديل الفهرست الحالي بناءً على التشابه بينه وبين الفهارس المجاورة له في الدليل. ولا بد من التنكير بأن الغاية الرئيسة من خوارزميات الكتابة المغطاة هي تضمين البيانات في الغطاء بصورة لا تثير الشك واستخلاص البيانات المضمنة بأعلى نسبة ممكنة من الدقة دون الاهتمام باسترجاع الغطاء وهذا ما يفسر اختلاف قيم PSNR بين الصورة الأصلية و stego-image بعد فك الكبس. واستطاعت الخوارزمية استخلاص البيانات المضمنة كاملة من دون أخطاء، كما هو واضح من قيم Bit Error Rate (BER). أما نتائج تضمين الصور فانظر الجدول (3).

جدول (3): نتائج تضمين صورة رمادية ذات امتداد BMP في صور رمادية.

BER	PSNR in dB			أبعاد الصورة السرية (Pixel)	الصورة السرية	بُعد المكتم الاتجاهي (Pixel)	الأبعاد (Pixel)	الصورة الأصلية
	بعد فك الكبس		بعد الكبس					
	الأصل/ stego	الأصل/ الغطاء	الغطاء/ Stego					
0	26.5806	35.3862	42.5113	54×54	Chess	4	376×500	Sunset. bmp
0	33.541	39.3344	42.9137	99×118	Girl	2		
0	28.1044	33.8709	42.5566	55×55	mandri	4	512×384	Vegetable. png
0	33.2455	38.4380	42.8118	110×11	Boats	2		
0	23.2451	29.5555	42.4108	66×62	bird	4	512×512	Sailboat. png
0	27.8609	34.8126	42.8357	128×12	moon	2		

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

وقد طبقت الخوارزمية على صور ملونة وكونت دليلاً منفصلاً لكل مستوى لوني ثم طبقت خوارزمية الكبس على كل مستوى لوني من المستويات الثلاثة كل على حدة، ثم دمجت المستويات الثلاثة مع بعضها للحصول على صورة الغطاء. وقد طبقت خوارزمية التضمين على مستوى لوني واحد وهو المستوى الأحمر إذ أن المستوى اللوني الأحمر كان أفضل نسبياً من المستويين الآخرين فيما يتعلق بقيمتي PSNR و BER. وكانت نتائج تطبيق تضمين نص في الصور الملونة كما في الجدول (4)

جدول (4): نتائج تضمين نص في صور ملونة

BER %	PSNR in dB		طول النص السري (Bit)	سعة التضمين القصى (Bit)	PSNR in dB الأصل/الغطاء	بُعد المكتم الاتجاهي (Pixel)	الأبعاد (Pixel)	الصورة الأصلية
	بعد فك الكبس	بعد الكبس						
	الأصل/stego	الغطاء/stego						
0.2	30.8343	55.5028	4096	8184	32.5686	4	256×256	Fish. bmp
0.9	35.5078	55.7448	16384	32760	36.9726	2		
0.008	31.5474	53.2137	25992	25992	32.8596	4	520×400	Vase.b mp
0.9	35.568	53.0373	103992	103992	37.5769	2		
0.4	27.5409	52.8937	8184	8184	31.3453	4	256×256	Fly. png
0.3	32.7418	53.0087	32760	32760	36.1837	2		

تم احتساب قيمة PSNR من خلال إيجاد معدل قيمها للمستويات اللونية الثلاثة فكانت قيمة PSNR بين الصورة الغطاء والصورة stego-image بعد الكبس تساوي Inf لأن عملية التضمين قد تمت على المستوى اللوني الأحمر فقط، ولغرض إثبات تلك القيمة فقد 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 جداً 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 فكانت كما هو مبين في الجدول (5)

جدول (5): نتائج تضمين صور رمادية ذات امتداد BMP في صور ملونة.

الصورة	الأبعاد	بُعد	الصورة	أبعاد	PSNR in dB	BER

%	بعد فك الكبس		بعد الكبس	الصورة السرية (Pixel)	السرية	المكم الاتجاهي (Pixel)	(Pixel)	الأصلية
	الأصل/ stego	الأصل/ الغطاء						
0.2	26.0418	28.2279	52.9592	30×34	Key	4	256×256	Jasmine. bmp
0.2	32.0003	33.7222	55.303	48×50	Boy	2		
0.06	25.4876	27.4651	53.1864	45×45	Bird	4	452×300	Penguin. bmp
0.2	30.3064	32.8619	53.264	91×91	Moon	2		
0.05	24.8029	26.8678	53.0964	30×34	Key	4	256×256	Pizza. png
0.09	29.9637	32.3525	53.1595	64×63	cartoon	2		

بلغت نسبة كبس أي صورة في الخوارزمية المقترحة (2 bpp) إذا كان بُعد المكمم الاتجاهي 2×2، وتزداد نسبة الكبس إلى (0.5 bpp) عندما يزداد بُعد المكمم الاتجاهي إلى 4×4. كما بلغت كفاءة تضمين الخوارزمية المقترحة 0.25 والمحسوبة بحسب المعادلة (11). وقد أجريت التجارب باستخدام نظام حاسوبي من نوع Pentium4 بمواصفات (RAM = 1 GB, CPU = 1.60 GHz)، وتراوح الزمن المستغرق في تضمين الحد الأعلى لعدد الخلايا الثنائية تقريباً بين: (1444 ثانية) لأكبر صورة رمادية ذات أبعاد (800×600) نقطة ضوئية وُبعد (2×2)، وبين: (62 ثانية) لأصغر صورة رمادية ذات أبعاد (256×256) نقطة ضوئية وُبعد (4×4). أما زمن استخلاص البيانات المضمنة في الصور المذكورة نفسها فتتراوح تقريباً بين (60 ثانية) و (1 ثانية) لأكبر صورة وأصغر صورة على التوالي. في حين تراوح الزمن المستغرق في الصور الملونة بين: (2019 ثانية) لأكبر صورة ملونة ذات أبعاد (606×4454) نقطة ضوئية وُبعد مكمم اتجاهي (2×2) وبين: (122 ثانية) لأصغر صورة ملونة ذات أبعاد (256×256) نقطة ضوئية وُبعد مكمم اتجاهي (4×4)، أما زمن استخلاص البيانات المضمنة في الصور المذكورة نفسها فتتراوح بين (31 ثانية) و (1 ثانية) لأكبر صورة وأصغر صورة على التوالي. ولا بد من الإشارة إلى أن الزمن المستغرق في التضمين تضمن 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.

11- 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 تنوعاً أكثر للأغطية المستخدمة في التضمين أكثر من الدليل العام لاسيما وأن الكتابة المغطاة تتطلب إرسال صورة مختلفة عن الصور السابقة في كل اتصال. وكان لبُعد المكمم الاتجاهي تأثيراً كبيراً على جودة الصورة وكمية البيانات المضمنة. كما إن إمكانية استخلاص البيانات المضمنة دون الحاجة لوجود الدليل كان لها الأثر الكبير في تقليل الزمن المستغرق في عملية الاستخلاص. وفيما يخص الصور الملونة فإن تطبيق التضمين على مستوى لوني واحد يحافظ بشكل كبير على جودة الصورة لأن التضمين سوف يؤثر على مستوى لوني واحد دون المستويين الآخرين.

المصادر

- [1] Amin F., Soleimanipour M., and Karimi A., (2008), "A Novel Plausible eniability Scheme in Secure Steganography", World Academy of Science, Engineering and Technology, Vol. 43, pp.217-219.
- [2] Ashok J. and Rajan E. D. G., (2010), "Principal Component Analysis Based Image Recognition", IJCSIT, Vol. 1, No. 2, pp: 44-50.
- [3] Chang C. C. and Wu C. W.,(2007), "Fast Planar-Oriented Ripple Search Algorithm for Hyperspace VQ Codebook", IEEE Transactions On Image Processing, Vol. 16, No. 6, pp.1538-1546.
- [4] 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
- [5] Chang C. C., Chen G. M., and Lin C. C., (2009), " Lossless Compression Schemes of Vector Quantization Indices Using State Codebook", Journal Of Software, Vol. 4, No. 4, pp.274-282.
- [6] 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.
- [7] Chang C.C., and Lin P.Y., (2004), "A Compression-Based Data Hiding Scheme Using Vector Quantization and Principal Component Analysis", International Conference on Cyberworlds, Tokyo, Japan.
- [8] Du W. C. and Hsu W. J., (2003), "Adaptive Data Hiding Based on VQ Compressed Images", IEE Proc.-Vis. Image Signal Process., Vol. 150, No. 4, pp. 233-238.
- [9] Hovancak R., Foris P., and Levicky D., (2006), " Steganography Based on DWT Transform", In: Radioelektronika (2006): 16th international Czech - Slovak scientific conference: Conference Proceedings. Bratislava. Slovak University of Technology, Czech.
- [10] Katzenbeisser S. C., and Petitcolas F. A. P., (2000), "Information hiding techniques for steganography and Digital Watermarking", Artech House, Bosten, London.
- [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] 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.
- [13] Motameni H., Norouzi M., Jahandar M., and Hatami A., (2007), "Labeling Method in Steganography", World Acad. Sci. Eng. Technol., Issue 30, pp. 349-354.
- [14] Potdar V., and Chang E., (2004), "Visibly Invisible: Ciphertext as a teganographic Carrier", 4th International Network Conference, Plymouth U.K.

- [15] Saffar H. E., (2008), "Channel Optimized Vector Quantization: Iterative Design Algorithms", MSc Thesis, Department of Mathematics and Statistics, Queen's University, Kingston, Ontario, Canada.
- [16] 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.
- [17] 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.

الملحق أ

نماذج من الصور التي أجريت عليها اختبارات الخوارزمية المقترحة

شكل (أ-1): تضمين نص في الصورة الرمادية (Child.bmp)

وبالسعة القصوى للتضمين، بعد المكتم = 4

(أ) الصورة الأصلية

(ج1) stego-image

(ج2) الصورة المسترجعة

(ب1) الغطاء

(ب2) الصورة السرية

(هـ) stego-image بعد فك الكيس

(د) الغطاء بعد فك الكيس

شكل (أ-2) تضمين صورة رمادية (Cartoon.bmp) في الصورة الملونة (Pizza.png)

بعد المكمم = 2