Hide Compressed Texts in an Audio File

Shahad Abdel-Rahman Hasso

College of Computer Science and Mathematics
University of Mosul, Mosul, Iraq

Received on: 15/10/2012 **Accepted on: 30/01/2013**

ABSTRACT

Steganography art is a technique of hiding data within data, as hiding text message within an image or an audio file or a video file, it is a new method used as a substitute for the known encryption technology.

This kind of hidden messages is distinguished that they reach their destination completely confidential, unlike encrypted messages that although it can never decoded without access to the encryption key; it can be identified as an encrypted message.

In this work, a new algorithm is proposed for compression and encodes the data using Huffman coding technique, then hides them in an audio file using a secret key for the distribution of encoded data within and LSB well known approach. The output is saved in a new audio file. In the recovery phase, the values are retrieved and decoded by the same method.

Results show highly accurate results as a measure auditory perception of the original file and the embedded data file as well as performance metrics knowledge (signal-to-noise ratio and the correlation coefficient and the mean square error and the peak signal to noise ratio).

Keywords: Steganography, hiding data, LSB approach, noise.

إخفاء النصوص المكبوسة في ملف صوتي

شهد عبد الرحمن حسو

كلية علوم الحاسوب والرياضيات

جامعة الموصل، الموصل، العراق

تاريخ استلام البحث: 2012/10/15 **تاريخ قبول البحث: 2013/01/30**

الملخص

يتلخص مبدأ تقنية فن الإخفاء في إخفاء البيانات ضمن بيانات، كإخفاء رسالة نصية ضمن صورة أو ملف صوتي أو ملف فيديو، وهي طريقة تستخدم بديلاً لتقنية التشفير المعروفة.

وما يميز هذا النوع من الرسائل المخفية هو أنها تصل إلى وجهتها بشكل سري تماماً، على خلاف الرسائل المشفرة التي على الرغم من أنه لا يمكن فك شفرتها من دون الحصول على مفتاح التشفير، فإنه بالإمكان تحديدها بوصفها رسالة مشفرة.

تم في هذا العمل اقتراح خوارزمية جديدة لكبس وترميز البيانات بطريقة هوفمان للترميز ثم إخفائها في ملف صوت باستخدام مفتاح سري لتوزيع البيانات المرمزة داخله وبطريقة LSB المعروفة. ثم يتم خزن الناتج في ملف صوت جديد. وفي مرحلة الاسترجاع يتم استرجاع القيم المرمزة وفك ترميزها بنفس طريقة الترميز.

أثبتت النتائج دقة عالية حسب مقياس الإدراك السمعي للملف الأصلي والملف المضمن بالبيانات وكذلك حسب مقاييس الأداء المعرفة (نسبة الإشارة إلى الضوضاء ومعامل الارتباط ومربع الخطأ وقمة إشارة الضوضاء).

الكلمات المفتاحية: إخفاء المعلومات، إخفاء البيانات، نهج LSB ، ضوضاء.

1- المقدمة:

بعد التطور الهائل الذي طرأ على تكنولوجيا المعلومات في مجال الاتصالات والإنترنت، ظهرت الحاجة إلى إيجاد وسائل لإيصال المعلومات والبيانات بصورة صحيحة ومنع الجهات غير المخولة من الإطلاع على هذه المعلومات، من هذه الوسائل التشفير وإخفاء البيانات (الرسائل) داخل الملفات الصورية أو الصوتية أو كلاهما معاُ (ملفات الفيديو) [1].

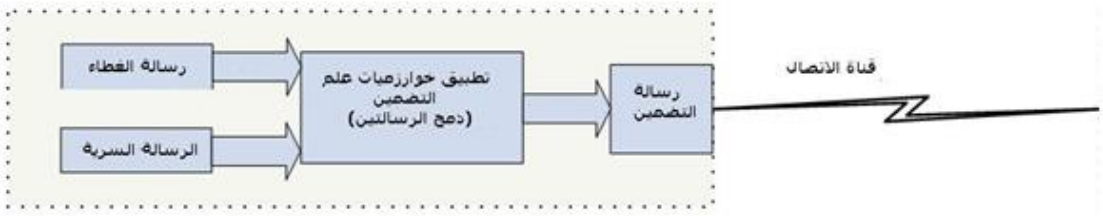
إخفاء المعلومات هي وسيلة لحجب البيانات السرية داخل ملفات الصور أو الصوت والفيديو والملفات القابلة للتنفيذ بحيث من غير الممكن لأي شخص باستثناء المرسل والمستلم أن يشك في وجود معلومات مخفية في ذلك الملف. ويمكن تطبيق الترميز لتغيير شكل البيانات وتوزيع محتوياتها بصيغة لا تثير الشكوك.

الميزة الرئيسية لإخفاء المعلومات في وسائل أخرى هي عدم إثارة الشكوك حتى لو سقطت في يد طرف ثالث.. على عكس الرسائل المشفرة، فستكون الرسائل بحد ذاتها وسيلة جذب انتباه الطرف الثالث [2].

على الرغم من أن تقنيات إخفاء المعلومات لها تطبيقات كثيرة مفيدة، لكنها قد تستخدم لأغراض غير مشروعة مثل إخفاء محتوى إباحي في غيرها من الملفات الكبيرة أو استخدام الإرهابيين لإخفاء المعلومات الخاصة بأعمال الشغب والاتصال لإخفاء معلوماتهم السرية والتعليمات.

كل ما تقدم يعد سبباَ رئيسياَ للتقدم الأوسع للكتابة المخفية مقارنةً بطرائق التشفير، لأن الكتابة المشفرة أو المشوهة تدفع المتابع إلى الخوض بشتى الوسائل للحصول على المعلومة الأصلية ومحاولة كسر الشفرة، في حين أن الكتابة المخفية لا تثير الشك عند المشاهد العادي، وقد يمر عليها مرور الكرام دون أن يترك أثرا للمعلومة المخفية داخل الملف المضمّن [3].

الإخفاء هو علم وفن تضمين البيانات المُراد إرسالها (قد تكون رسائل نصّية أو صورية) داخل بيانات مُرسلة (قد تكون صوراً أو ملفات الصوت أو الفيديو، وذلك لاحتوائها على كمية كافية من البيانات التي تُمكّن المستخدم من إخفاء البيانات داخلها) وكما مبين في الشكل (1) [1].



الشكل (1). تقنية إخفاء المعلومات

2- الهدف من البحث:

قدم عدد كبير من الباحثين دراسات في مجال الإخفاء وكذلك في مجال كبس البيانات ولكن قليلاً منهم تطرق إلى إخفاء البيانات المكبوسة حيث إن الملف الغطاء عادة يكون اكبر بكثير من الرسالة المراد إخفاءها لذا لا تحتاج إلى كبس البيانات وهنا تأتي أهمية البحث في معالجة البيانات وتقليل حجمها بواسطة خوارزمية هوفمان ثم إخفائها في ملف صوت وسبب اختيار طريقة هوفمان بالذات لأنها تقوم بترميز البيانات ليس فقط للتقليل من حجمها ولكن أيضا لزيادة سريتها عن طريق الكبس حيث إن الشخص غير المخول لن يستطيع الوصول إلى النص الصريح بسبب ترميز البيانات المطبق قبل إخفائها. بالإضافة إلى ذلك زيادة حجم البيانات المخفية داخل ملف الصوت.

3- الدراسات السابقة

قدم Jithendra وSen-ching (2008) [9] طريقة جديدة لكبس البيانات وإخفائها في ملفات الفيديو بعد تحديد طريقة التضمين المثلى optimal embedding strategy للتقليل من الإدراك الحسي للملفات وكذلك معدل بت الإخراج Bit Rate. تُضمّن البيانات في معاملات تحويل جيب التمام المتقطع (Discrete Cosine Transform) والتي توجد في معظم ملفات الفيديو ويتم اختيار المعاملات اعتمادا على التقليل من الكلفة التي تجمع بين كل من التشويه ومعدل البت.

أما Niladri وآخرون (2009) [10] فقاموا باقتراح طريقة جديدة لتضمين والاسترجاع Localization and restoration العلامة المائية باستخدام الوحدة الصورية pixel للضوضاء في الصور الثنائية. تم التمكن من استرجاع الصور حتى بعد إجراء بعض المعالجات عليها مثل التكبير والتصغير والتدوير و... الخ.

اقترح الدكتور لؤي جورج وآخرون (2010) [11] طريقتين جديدتين لإخفاء البيانات السرية في ملف صوتي. الأولى عن طريق تعديل سعة عينات الملف الصوتي والتي حققت نسبة جيدة من الإخفاء لكنها لم تستطع الصمود أمام التغيرات التي تحصل على الملفات مثل الكبس. أما الطريقة الثانية فقد صممت لإخفاء بيانات لها القدرة على الصمود أمام التغيرات التي يتعرض لها الصوت وذلك بالاستفادة من بعض المناطق الصوتية واللاصوتية في الملفات.

وقام R.S. AARTHI وآخرون (2012) [12] باقتراح طريقة تحل مشكلة زيادة التعقيد في تصميم وتصنيع التكنولوجيا الحديثة والمستخدمة اختبار حجم البيانات. لتقليل حجم بيانات الاختبار، تم اقتراح عدة تقنيات تعتمد على تقنية هوفمان المعروفة. وقد أعطت الطرائق المقترحة نسبة كبس عالية وتقليلاً كبيراً في حجم البيانات المخزونة.

4- لمحة تاريخية لفن الإخفاء

تخبرنا المعلومات إن علم إخفاء المعلومات في بداياته يعود إلى سنة 440 قبل الميلاد حين قام القائد (هيستوريوس) بحلق رأس احد خدامه الموثوق بهم ووشم على رأسه رسالة اختفت بعد أن نمى شعره عليها وكان الغرض من هذه العملية تحريك العصيان ضد خصمه (بيرسيناس) والطريقة المذكورة ظلت مستخدمه من قبل الألمان حتى بداية القرن العشرين.

وبعد ذلك بفترة طويلة وبالتحديد في بداية القرن الخامس عشر الميلادي اكتشفت شبكة كاردا نو المستطيلة والمثقبة بطريقة عشوائية وغير منظمة توضع هذه الشبكة على الورقة وتكتب الرسالة السرية على هيئة أحرف أو

كلمات من خلال الثقوب بعد ذلك تملئ الفراغات المتروكة برسالة تغطي الرسالة السرية وبشكل غير مؤذي لها لكي تظهر بمظهر رسالة عادية وبريئة ومن ثم ترسل إلى الطرف الأخر الذي لديه الشبكة نفسها فيضعها على الورقة ليستخلص الرسالة السرية.

وهناك إعداد كبيرة من التقنيات اخترعت في فن إخفاء المعلومات تتضمن إخفاء رسائل في بعض الإشكال من المراسلات والنصوص المكتوبة على الألواح الخشبية والملاحظات المحمولة بواسطة الحمام الزاجل. كما استخدمت آلية تغيير ارتفاع الحروف في النص أو عمل فتحات صغيرة فوق أو تحت الحروف في النص وهذه التقنية في التراسل ظلت مستخدمه في القرن السابع عشر ولكن طورت من قبل (ويل كنيس) عام -1614) (1672والذي استخدم الحبر المخفي غير المرئي لطبع نقاط صغيرة بدلا من التعليم بواسطة الفراغات وقد أعيد استخدامها مرة أخرى من قبل الألمان خلال الحربين العالميتين الأولى والثانية، والتبني الحديث لهذه التقنية ظل مستخدما لضمان سرية الوثائق حتى الآن.

في عام 1860 تم حل المشاكل الرئيسية لعمل صور صغيرة من قبل (دارجون) وهو مصور فوتوغرافي فرنسي عمل في الحرب عام 1870-1871 حينما كانت باريس محاصرة وقام بإرسال الرسائل على الأفلام الفوتوغرافية وكانت ترسل مع الحمام الزاجل [4].

5- متطلبات إخفاء المعلومات:

هناك عدة تقنيات تضمين تمكننا من إخفاء المعلومات في شيء معين وجميع وهذه التقنيات يجب أن تحقق عددا من المتطلبات لكي يمكن تطبيق نظرية إخفاء المعلومات بصورة صحيحة [4] من هذه المتطلبات:

- ❖ الإكمال الصحيح للمعلومات المخفية لدى تضمينها داخل الغطاء بحيث أن الرسالة السرية يجب أن لا تتغير بأي طريقه في حاله إضافة معلومات أو تغيير أية معلومات مضمنه بعد إخفائها وان تغيير البيانات المضمنة يعني فشل العملية.
- ❖ يجب أن لا يتغير الوسط الناقل الذي يغطي الرسالة السرية أيضا وعلى الأقل أن لا تكون تغييراته ظاهرة للعيان وفي حالة كون التغييرات على الوسط الناقل كبيرة وظاهرة للعيان فان الشخص الذي يشاهدها سوف يعلم بأن هناك معلومات مخفيه داخلها فيحاول أن يفتحها أو يدمرها.
- ❖ يؤخذ بنظر الاعتبار دائما أن المهاجم يعرف بوجود معلومات مخفية داخل الغطاء.

6- أساليب الإخفاء

بشكل عام يمكن تقسيم أساليب الإخفاء إلى أربعة أساليب أساسية وهي [2][3]:

- ❖ الإخفاء النصي
- ❖ الإخفاء الصوتي
- ❖ الإخفاء الفيديوي
- ❖ الإخفاء الصوري

7- خوارزمية الإخفاء بالبت الأقل أهمية Least Significant Bit

هي أكثر الطرائق المستخدمة في الإخفاء شيوعا وتطبيقا حيث تقضي بإدخال بت أو أكثر من الرسالة المراد إخفاؤها وإبداله بالبت ذي أقل أهمية من الصوت [5]. البت الأقل أهمية هو البت الذي له اقل قيمة حسابية $(2^0=1)$.

يتم إخفاء البيانات في ملف الصوت عادة في مجال الوقت (time domain) بـ LSB حيث يختار مجموعة فرعية من جميع عينات ملف الصوت الغطاء والتي اختارها مفتاحاً سرياً. يتم تنفيذ العملية باستبدال LSBs من هذه المجموعة الفرعية ليوضع بدله بت من الملف المراد إخفاءه. وتتم عملية الاسترجاع من خلال قراءة المجاميع من الصوت الغطاء (stego). [5]

1-7 الخطوات الرئيسية لخوارزمية LSB [6]:

- **الإخفاء**

1- قراءة ملف الغطاء وقراءة الملف المراد إخفاؤه.
2- تحويل الملف المراد إخفاءه إلى الصيغة الثنائية.
3- حساب البت الأقل أهمية في ملف الغطاء وتحديده.
4- تبديل البت الأقل أهمية في ملف الغطاء ببت من الملف المراد إخفاءه واحد بواحد.
5- خزن الناتج في ملف جديد بنفس نوع ملف الغطاء (صورة أو صوت أو فيديو).

- **الاسترجاع**

1- قراءة ملف الغطاء.
2- حساب البت الأقل أهمية في ملف الغطاء وتحديده.
3- استرجاع البت الأقل أهمية في ملف الغطاء.
4- تحويل مجموعة البت إلى صيغتها الرقمية (في حالة النص مثلا كل 8 بت تحول إلى حرف وهكذا).

8- كبس البيانات Data Compression:

كبس البيانات هي عملية تقليل المساحة الخزنية للملفات التي تحوي هذه البيانات. هناك العديد من خوارزميات كبس البيانات والتي تقوم بكبس بيانات مختلفة الأشكال. وكذلك هناك عدد من خوارزميات الكبس المختلفة يمكن استخدامها لكبس نوع واحد من البيانات. ويستخدم كبس البيانات على نطاق واسع في تطبيقات عديدة ومتنوعة.

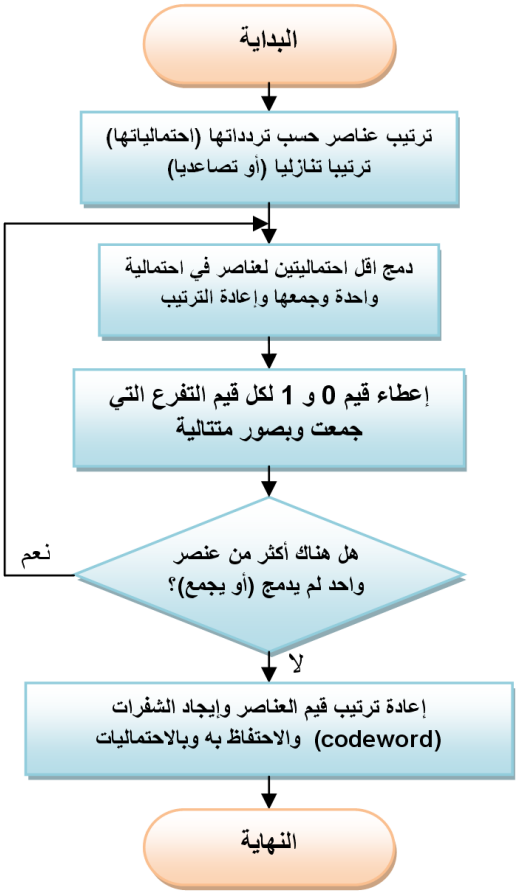
الكبس هو فن تمثيل المعلومات في شكل مكبوس بدلا من الأصلي، هذا مفيد جدا في معالجة وتخزين أو نقل الملفات الضخمة التي تحتاج إلى كثير من الأجهزة. عند استخدام كبس البيانات في تطبيق نقل البيانات فان سرعة النقل هي الهدف الأساسي، أما في تطبيق تخزين البيانات فان نسبة الكبس هي الهدف الأساس.

يمكن تصنيف كبس البيانات على أنها إما كبس بضياع Lossy compression أو عدم ضياع Lossless compression. تقنيات الكبس بعدم ضياع هي عملية إعادة بناء البيانات الأصلية من الملف المكبوس من دون أي فقدان للبيانات. ويطلق على هذا النوع من خوارزميات الكبس بالخوارزميات العكسية (reversible algorithm) وتستخدم لكبس الصور الطبية والنصوص والصور والملفات القابلة للتنفيذ وغير ذلك. وهناك الكثير من خوارزميات الكبس بدون ضياع.

تقنيات كبس البيانات بضياع تقوم بإعادة بناء الرسالة الأصلية مع فقدان بعض المعلومات. مثل هذه التقنيات يمكن أن تستخدم في الوسائط المتعددة للفيديو والصور والصوت لتحقيق كبس البيانات [7].

9- خوارزمية هوفمان للترميز Huffman Coding Algorithm

يتم تعيين رمز هوفمان من طول ثابت لترميز البيانات إلى طول متغير. تبدأ خوارزمية هوفمان استنادا إلى قائمة البيانات التي يتم ترتيبها تنازلي حسب احتمالات ورودها في الملف المراد ترميزه. ثم يتم إنشاء شجرة ثنائية بطريقة أسفل – أعلى bottom-up مع رمز في كل ورقة. هذه العملية تتم بعدة خطوات في كل خطوة يتم اختيار البيانات ذات الترددات الأقل وتضاف إلى الجزء العلوي من الشجرة الجزئية ثم يتم حذف الترددات الأصغر المختارة من القائمة والتي حلت محلها قيم ثانوية تدل على اثنين من القيم الأصلية. وبهذه الطريقة يتم تقليل القائمة لقيمة واحدة ثانوية. وهكذا تستمر العملية لحين الحصول على قيمة واحدة فقط. وأخيرا يتم تعيين رمز لكل ورقة يعتمد على المسار من العقدة الجذر إلى الرموز في القائمة وكما مبين في الشكل (2) والذي يوضح المخطط الانسيابي لخوارزمية هوفمان للترميز [8].



الشكل (2). المخطط الانسيابي لخوارزمية هوفمان للترميز

10- الخوارزمية المقترحة:

- **الإخفاء:** تتم عملية إخفاء البيانات عن طريق إجراء الخطوات الآتية:

1- قراءة ملف الصوت وتحديد طول الملف (عدد العينات الكلي) ونسبة العينات Sample Rate.

2- عن طريق معرفة معلومات ملف الصوت نجد مفتاح خزن البيانات داخل ملف الصوت وكالاتي:

$$key = \frac{number\ of\ \ samples}{sample\ rate}$$

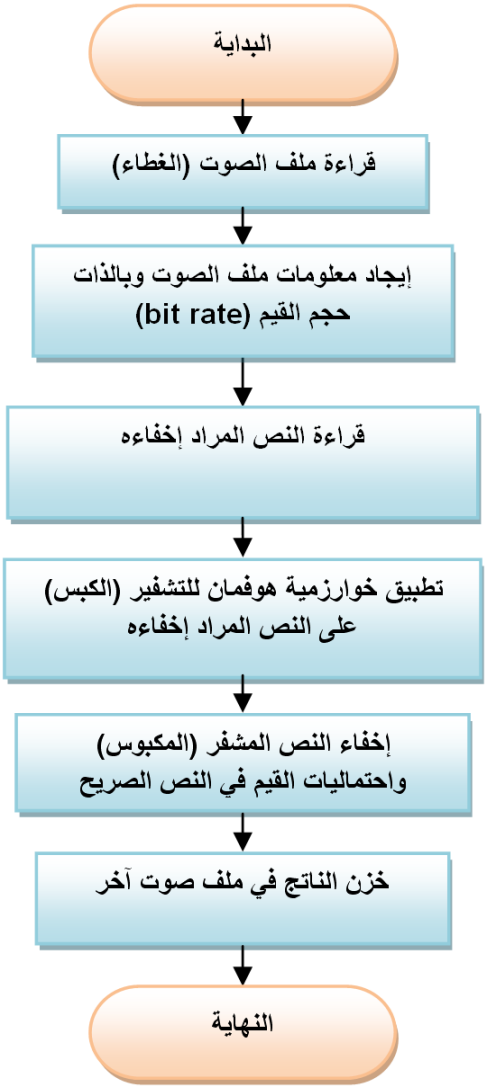
3- قراءة ملف النص.

4- تطبيق خوارزمية هوفمان للترميز على ملف النص وبذلك سوف يتم تحويل النص إلى سلسلة من البت.

5- لكل قيمة في ملف الصوت بدل القيمة في الموقع LSB بقيم احتماليات أحرف ورموز النص الصريح ثم بنتائج ترميز النص في الخطوة السابقة وباستخدام المفتاح.

6- إنشاء ملف صوت جديد (يحتوي على ناتج تضمين النص داخل ملف الصوت).

والشكل (3) يوضح المخطط الانسيابي لخوارزمية الإخفاء المقترحة



الشكل (3). المخطط الانسيابي لخوارزمية الإخفاء المقترحة

- **الإظهار (الاسترجاع):** تتم عملية استرجاع البيانات من ملف الصوت عن طريق إجراء الخطوات الآتية:

1- قراءة ملف الصوت المخفي فيه نص وتحديد طول الملف (عدد العينات الكلي) ونسبة العينات Sample Rate.

2- عن طريق معرفة معلومات ملف الصوت نجد مفتاح خزن البيانات داخل ملف الصوت وكالاتي:

$$key = \frac{number\ of\ \ samples}{sample\ rate}$$

3- استرجاع القيم التي تحتوي على ترددات الأحرف والرموز في النص.

4- قراءة واسترجاع كل قيمة في ملف الصوت في LSB في موقع وحسب المفتاح.

5- تطبيق خوارزمية هوفمان لفك الترميز على القيم المسترجعة لغرض الحصول على النص الصريح.

6- خزن الأحرف والرموز المسترجعة في ملف نصي.

11- النتائج

1- تم تنفيذ الخوارزمية المقترحة على مجموعة مختلفة من ملفات الصوت ذات الامتداد (.wav) وكانت النتائج ناجحة في الوصول إلى الهدف المطلوب وبجودة عالية، وقد تم اعتماد مقاييس الأداء نسبة الإشارة إلى الضوضاء Signal to Noise Ratio (SNR) وقمة معدل الضوضاء Peak SNR (PSNR) وقيمة معامل الارتباط Correlation ومعدل مربع الخطأ Mean Square Error (MSE) وفقا للمعادلات (1) إلى (4) لتقييم أداء الخوارزمية المقترحة وكما مبين في الجداول من (1) إلى (6) والتي تبين نتائج تطبيق الخوارزمية المقترحة على أحجام مختلفة من ملفات الغطاء والنصوص المراد إخفاؤها ونسبة الإشارة إلى الضوضاء ومعامل الارتباط لهذه الملفات.

$$SNR_{db} = 10\log 10\left[\frac{\sum (I)^2}{\sum (O-I)^2}\right] \quad \ldots(1)$$

$$corr = \frac{\sum (I-\mu_I)(O-\mu_O)}{\sqrt{\sum (I-\mu_I)^2 \sum (O-\mu_O)^2}} \quad \ldots(2)$$

$$PSNR = 10\log 10\left[\frac{\max value(I,O)^2}{abs(O-I)^2}\right] \quad \ldots(3)$$

$$MSE = \frac{1}{M}\sum (O-I)^2 \quad \ldots(4)$$

حيث I تمثل بيانات الصوت المدخلة وO تمثل بيانات الصوت الحاوي على البيانات المخفية

M عدد العينات (البيانات)

μ معدل العينات

2- تم تقييم العمل عن طريق الإدراك السمعي للملفات الصوتية المضمنة مقارنة مع الملف الأصلي ولم يظهر أي اختلاف سمعيا بين الملفين.

3- تم استرجاع كافة الملفات النصية المخفية بنسبة 100% بعد تطبيق خوارزمية هوفمان لفك الكبس.

الجدول رقم (1): مقاييس الأداء بعد تطبيق الخوارزمية المقترحة على نص مكون من 66 رمز (بضمنها الأحرف) وبعدد 273 بت بعد تطبيق الكبس

File No.	File Size(KB)	SNR	MSE	PSNR	Correlation
1	1,741	35.015974	0.000001	60.513998	0.999685
2	1,653	26.104120	0.000011	42.947102	0.997545
3	1,643	34.791587	0.000000	53.907921	0.999668
4	1,277	29.879011	0.000014	44.205364	0.998971
5	1,235	33.762702	0.000001	55.187963	0.999579
6	1,059	27.742617	0.000017	47.530772	0.998490
7	1,002	18.740722	0.000060	40.359737	0.987022
8	999	31.225192	0.000021	46.695243	0.999237
9	983	27.751828	0.000025	45.753937	0.997617
10	868	21.504680	0.000000	39.588040	0.992769
11	851	32.326990	0.000004	48.661595	0.999420
12	830	16.710568	0.000033	41.319283	0.978440

الجدول رقم (2): مقاييس الأداء بعد تطبيق الخوارزمية المقترحة على نص مكون من 269 رمز (بضمنها الأحرف) وبعدد 1120 بت بعد تطبيق الكبس

File No.	File Size(KB)	SNR	MSE	PSNR	Correlation
1	1,741	31.243559	0.000002	56.741584	0.999249
2	1,653	22.464607	0.000025	39.307589	0.994314
3	1,643	28.925521	0.000002	48.041855	0.998719
4	1,277	22.768411	0.000070	37.094764	0.994700
5	1,235	29.994250	0.000003	51.419510	0.998998
6	1,059	25.443732	0.000029	45.231887	0.997434
7	1,002	18.562136	0.000062	40.181151	0.986473
8	999	22.017795	0.000178	37.487846	0.993628
9	983	24.137858	0.000057	42.139967	0.994515
10	868	16.636215	0.000000	34.719576	0.977743
11	851	26.273136	0.000017	42.607741	0.997662
12	830	11.747588	0.000102	36.356303	0.930729

الجدول رقم (3): مقاييس الأداء بعد تطبيق الخوارزمية المقترحة على نص مكون من 535 رمز (بضمنها الأحرف) وبعدد 2222 بت بعد تطبيق الكبس

File No.	File Size(KB)	SNR	MSE	PSNR	Correlation
1	1,741	28.923698	0.000003	54.421723	0.998718
2	1,653	19.637217	0.000049	36.480199	0.989069
3	1,643	26.978578	0.000003	46.094912	0.997993
4	1,277	19.338955	0.000155	33.665308	0.988287
5	1,235	28.278882	0.000005	49.704142	0.998513
6	1,059	25.213171	0.000030	45.001326	0.997294
7	1,002	18.544692	0.000062	40.163707	0.986419
8	999	20.017598	0.000283	35.487650	0.989881
9	983	22.251216	0.000088	40.253325	0.991518
10	868	14.173714	0.000001	32.257075	0.960696
11	851	23.169234	0.000034	39.503839	0.995215
12	830	10.958424	0.000123	35.567138	0.916301

الجدول رقم (4): مقاييس الأداء بعد تطبيق الخوارزمية المقترحة على نص مكون من 1420 رمز (بضمنها الأحرف) وبعدد 6185 بت بعد تطبيق الكبس

File No.	File Size(KB)	SNR	MSE	PSNR	Correlation
1	1,741	24.257942	0.000008	49.755966	0.996242
2	1,653	16.423702	0.000102	33.266685	0.976951
3	1,643	23.303255	0.000006	42.419589	0.995317
4	1,277	16.076550	0.000329	30.402903	0.975008
5	1,235	19.393009	0.000036	40.818270	0.988434
6	1,059	19.454154	0.000114	39.242309	0.989771
7	1,002	18.484468	0.000063	40.103483	0.986229
8	999	19.551666	0.000315	35.021717	0.988729
9	983	20.192847	0.000141	38.194955	0.986340
10	868	10.623028	0.000001	28.706389	0.911369
11	851	15.098839	0.000218	31.433444	0.968909
12	830	10.297700	0.000143	34.906414	0.901811

الجدول رقم (5): مقاييس الأداء بعد تطبيق الخوارزمية المقترحة على نص مكون من 2254 رمز (بضمنها الأحرف) وبعدد 9775 بت بعد تطبيق الكبس

File No.	File Size(KB)	SNR	MSE	PSNR	Correlation
1	1,741	22.043200	0.000014	47.541224	0.993736
2	1,653	15.308044	0.000132	32.151027	0.970097
3	1,643	19.061340	0.000016	38.177673	0.987514
4	1,277	14.950814	0.000426	29.277167	0.967489
5	1,235	16.825233	0.000066	38.250493	0.979011
6	1,059	18.198208	0.000152	37.986363	0.986318
7	1,002	15.496551	0.000126	37.115566	0.972408
8	999	19.521094	0.000317	34.991146	0.988649
9	983	17.346269	0.000272	35.348377	0.973520
10	868	9.123154	0.000002	27.206514	0.876754
11	851	12.666082	0.000382	29.000687	0.944889
12	830	10.017651	0.000152	34.626366	0.894898

الجدول رقم (6): مقاييس الأداء بعد تطبيق الخوارزمية المقترحة على نص مكون من 2589 رمز (بضمنها الأحرف) وبعدد 11197 بت بعد تطبيق الكبس

File No.	File Size(KB)	SNR	MSE	PSNR	Correlation
1	1,741	21.345386	0.000016	46.843410	0.992640
2	1,653	14.973731	0.000142	31.816714	0.967664
3	1,643	18.373708	0.000018	37.490042	0.985357
4	1,277	14.906279	0.000430	29.232632	0.967149
5	1,235	16.523313	0.000070	37.948574	0.977483
6	1,059	17.694070	0.000171	37.482225	0.984621
7	1,002	15.485905	0.000126	37.104921	0.972340
8	999	19.519916	0.000317	34.989968	0.988646
9	983	16.626448	0.000322	34.628556	0.968668
10	868	8.686226	0.000002	26.769587	0.864771
11	851	11.891163	0.000457	28.225768	0.933745
12	830	9.905336	0.000156	34.514050	0.891984

12- الاستنتاجات:

- ❖ لم تكن الفائدة من عملية كبس البيانات فقط لتقليل حجم البيانات لغرض خزنها أو نقلها بل لزيادة أمنية المعلومات الموجودة داخل الملفات النصية ومنع غير المخول من الوصول إلى المعلومات الصريحة حتى لو حصل شك بوجود معلومات.
- ❖ التعامل مع ملف الصوت يزيد من كفاءة الإخفاء وذلك لان زيادة حجم ملف الغطاء تزيد من أمنية البيانات مهما زاد حجم البيانات وكما هو واضح في الجدول رقم 6.
- ❖ أبدت الطريقة المقترحة كفاءة ودقة أداء عالية سمعيا وحسابيا وبتغير حجم النص المراد إخفاؤه وكما مبين في جداول النتائج إذ أنه مهما ازداد حجم النص المخفي فان قيم نسب الأداء تبقى ضمن مدى المعقول والمنطقي.

المصادر

[1] Barazenchi Fawzi A. Z., (2008), "*Hiding Data within Images*", book University of Sulymania, Iraq.

[2] Stallings William; (2006), "*Cryptography and Network Security Principles and Practices*", 4th Edition, Pearson Education, Inc., Prentice Hall.

[3] Socek Daniel, Hari Kalva, Spyros S. Magliveras, Oge Marques, Dubravko Culibrk, Borko Furht; (2007): "*New Approaches To Encryption And Steganography For Digital Videos*", Springer-Verlag.

[4] IRAQ Systems for Programming and Technical Solutions (2009), "*Data Hiding*", http://forums.iraqcst.com/showthread.php?t=8039

[5] Nedeljko Cvejic and Tapio Sepp Äanen, (2011), "*Increasing Robustness of LSB Audio Steganography by Reduced Distortion LSB Coding*", MediaTeam, Information Processing Laboratory, University of Oulu, Finland.

[6] Shami Jhodge, Girija Chiddarwar and Neha Pharande, (2012), "*Metamorphosis of High Capacity Steganography Schemes*", International Conference on Computer Networks and Communication Systems (CNCS), IPCSIT vol.35 (2012).

[7] Anuj Sharma & Mahendra Pratap Panigrahy, (2012), "*Neural Networks and Image Compression*", VSRD International Journal of CS & IT Vol. 2 (9), VSRD-IJCSIT, Vol. 2 (9), 2012, 746-755.

[8] Asadollah Shahbahrami, Ramin Bahrampour, Mobin Sabbaghi Rostami and Mostafa Ayoubi Mobarhan, (2011), "*Evaluation of Huffman and Arithmetic Algorithms for Multimedia*", Compression Standards , Faculty of Engineering, University of Guilan, Rasht, Iran.

[9] Jithendra K. Paruchuri and Sen-ching Samson Cheung (2008), "*Joint Optimization of Data Hiding and Video Compression*", Circuits and Systems, 2008. ISCAS 2008. IEEE International Symposium on, Date of Conference: 18-21 May 2008, Pp. 3021 - 3024

[10] Niladri B., Puhan Anthony T.S. Ho, and Farook Sattar, (2009), "*Localization and text sequence restoration using noise pixels in binary document image watermarking*", Journal of Electronic Imaging 18(2), 023012 (Apr–Jun 2009).

[11] Dr. Loay. A. Jorj, Dr. Hilal H. Saleh and Dr. Nidaa F.Hassan, (2010), "*Data Hiding in Audio File by Modulating Amplitude*", Eng. & Tech. Journal, Vol. 5, No. 28.

[12] R.S. Aarthi, D. Muralidharan, and P. Swaminathan, (2012), "*Double Compression of Test Data Using Huffman Code*", Journal of Theoretical and Applied Information Technology, 15 May 2012, Vol. 39, No. 2.