Use the Frequency Domain to Hide in Some Audio Files

Zahraa Tarik *zahraata.eng@uomosul.edu.iq*
College of engineering
University of Mosul

Farah T. Mohammd *farahtarik@uomosul.edu.iq*
College of computer science and mathematics
University of Mosul

Ikhlass Thanoon **Azhar Rafie**

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

ABSTRACT

In this work, anew hiding algorithm is proposed that depends on using two deferent domain (spatial and frequency) to achieve and provide security and protection for transformed data, which is represented in a text message encrypted using a key of direct standard method, then spatial domain were use to hide it inside an audio file, Using Discrete cosine transform (DCT) this file has been hidden inside a host audio file. The data of the text message has been fully retrieved after decrypting process, the value of normalization correlation is equal to one.

Key word: DCT, Audio, SNR, NC

استخدام المجال الترددي للإخفاء في بعض ملفات الصوت

زهراء طارق محمد *كلية الهندسة* *جامعة الموصل*

فرح طارق محمد **إخلاص خالد ذنون** **أزهار رافع عبد الله** *كلية علوم الحاسوب والرياضيات* *جامعة الموصل*

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

الملخص

تم في هذا العمل اقتراح خوارزمية تعتمد على استخدام مجالين مختلفين للإخفاء (المجال المكاني والمجال الترددي) لتحقيق وتوفير أمنية وحماية للبيانات المنقولة والمتمثلة في رسالة نصية مشفرة باستخدام مفتاح مدخل بطريقة Direct standard وقد تم اعتماد المجال المكاني في لإخفائها داخل ملف صوتي وباستخدام تحويل الجيب تمام المتقطع Discrete cosine transform (DCT) تَم إخفاء هذا الملف داخل ملف صوتي مضيف، وقد تم استرجاع بيانات الرسالة النصية بصورة كاملة بعد عملية فك الشفرة وكانت قيمة معامل الارتباط التعياري لها يساوي واحد.

الكلمات المفتاحية: ملفات الصوت، تحويل الجيب تمام المتقطع.

1. المقدمة:

إن لإخفاء البيانات أهمية كبيرة للحفاظ على المعلومات الحقيقية وعدم ظهورها للعيان أياً كان نوعها ويعتبر عاملاً مساعداً في إضافة حماية لها من القراءة أو العبث أو التدمير. يُستخدم هذا الفن في عدد من المجالات إلا أن المجال الذي يبرز فيه هذا الفن هو التجارة الإلكترونية التي تزداد تطبيقاتها، والاهتمام بها يومًا بعد آخر. من تطبيقات هذا العلم، العلامات المائية (Watermarks) والتي تستخدم في عمليات حفظ الحقوق للمنتجات الرقمية،والحد من عمليات القرصنة.وبالرغم من أن المشتري أو مستخدم هذه البرامج قد يعلم بوجود مثل هذه العلامات،إلا أن من الصعب اكتشاف أماكنها داخل الملف .وعلى افتراض أن المستخدم قد تعرف على مكان وجود هذه العلامة، فسيظهر أمامه تحدٍ آخر، وهو معرفة الطريقة المستخدمة في الإخفاء وكلمة السر ومفتاح التشفير، وكلا من هذه الأشياء قد يستغرق اكتشافه وقتاً زمنياً طويلاً[1][2].

ومن الدراسات السابقة قام الباحث Jixin Lui باعتماد خوارزمية العلامة المائية الصوتية المتعددة الأغراض ثم تقييمها بالاعتماد على مبدأ Vector quantization الذي اعتمد على تحويل الجيب تمام المتقطع[3]، كما قام الباحثان Nidhi H Divecha وN N Jani باقتراح خوارزمية تجمع بين مزايا التحويلات الثلاثة DWT، وDCT وSVD للصور الرقمية لتكون ضد كل أنواع الهجمات كون لديها قدرة عالية جدا على إخفاء البيانات[4].

2. طرق الإخفاء :

يمكن اعتماد المجال المكاني والترددي في الإخفاء، حيث يمكن إخفاء بيانات النص المشفر داخل الملف الصوتي الأول باستخدام LSB فمثلاً لإخفاء حرف 'E' يتم تحويله إلى سلسلة من الأرقام الثنائية وبما أن كل sample ممثل بـ8-bit، لذا يتم تغيير الـbit الأول أو الثاني حسب الخوارزمية ويعوض عنها بأحد أرقام السلسلة [5]. بعد تكوين الملف الوسطي يتم استخدام المجال الترددي باعتماد تحويل الجيب تمام المتقطع DCT للإخفاء في الملف الصوتي المضيف حيث يتم تقسيم الملف إلى مجموعة من الـframes(8sample/frame) وبإيجاد الـDCT لها كما في المعادلة[6]:

$$Y(k)=w(k)\sum_{n=1}^{N} x(n)\left(\cos \quad \frac{\pi(2n-1)(k-1)}{2N}\right) \qquad \ldots(1)$$

Where: K=1,2,…N

$$w(k)=\begin{cases}\frac{1}{\sqrt{N}}, & k=1\\ \sqrt{\frac{2}{N}}, & 2\le k\le N\end{cases}$$

ثم يتم إخفاء bit واحد في كل frame وعن طريق الاتفاق بين الطرفين يتم تحديد المعاملات التي يتم استخدامها في عملية التضمين حيث يتم الحفاظ عليها ومن ثم إجراء (IDCT) أي تحويل جيب تمام المعاكس لكل frame كما في المعادلة[7]:

$$X(n)=\sum_{k=1}^{N} y(k)*w(k)\left(\cos \quad \frac{\pi(2n-1)(k-1)}{2N}\right) \qquad \ldots(2)$$

Where :n=1, 2, ……N.

$$w(k)=\begin{cases}\frac{1}{\sqrt{N}}, & k=1\\ \sqrt{\frac{2}{N}}, & 2\le k\le N\end{cases}$$

3. الخوارزمية المقترحة:

تتمثل الخوارزمية المقترحة في إخفاء نص مشفر باستخدام طريقة الـ Direct standerd أو Caesar cipher لتشفير وفك شفرة البيانات النصية، تستخدم المعادلة C=(M+K) mod 26 للتشفير، أما لفك تشفير البيانات النصية فتم استخدام المعادلة M=(C-K) [8] عن طريق مفتاح مدخل ثم الإخفاء داخل ملف صوتي باستخدام LSB حيث تم الإخفاء في الـbit الأول لكل sample من موقع متفق عليه من قبل الطرفين وبعد إخفاء النص وتحويل الملف الصوتي الأول إلى سلسلة من الأرقام الثنائية يتم تحويل الملف الصوتي الثاني باستخدام تحويل جيب تمام المتقطع DCT، حيث يتم تقسيم الملف إلى مجموعة من الـframes كل مقطع بحجم (1*8 samples) وإخفاء بيانات الملف الصوتي الأول بحيث يتم إخفاء bit واحد لكلframes ثم إيجاد IDCT(أي تحويل جيب تمام المتقطع المعاكس) وقد

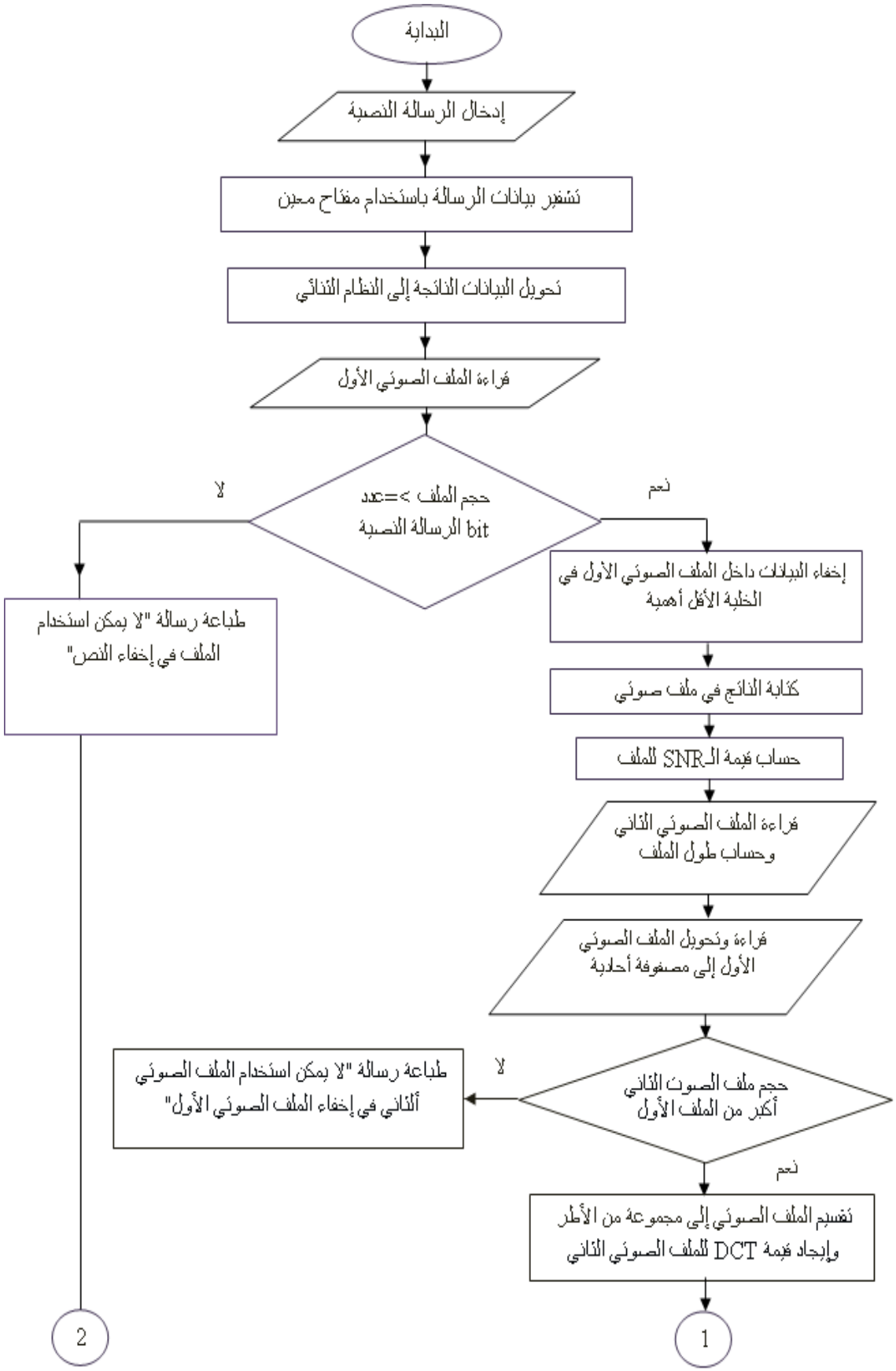
تم إخفاء عدد حروف الرسالة وقيمة المفتاح وحجم الملف الصوتي الثاني في مواقع متفق عليها من أجل استرجاع البيانات.

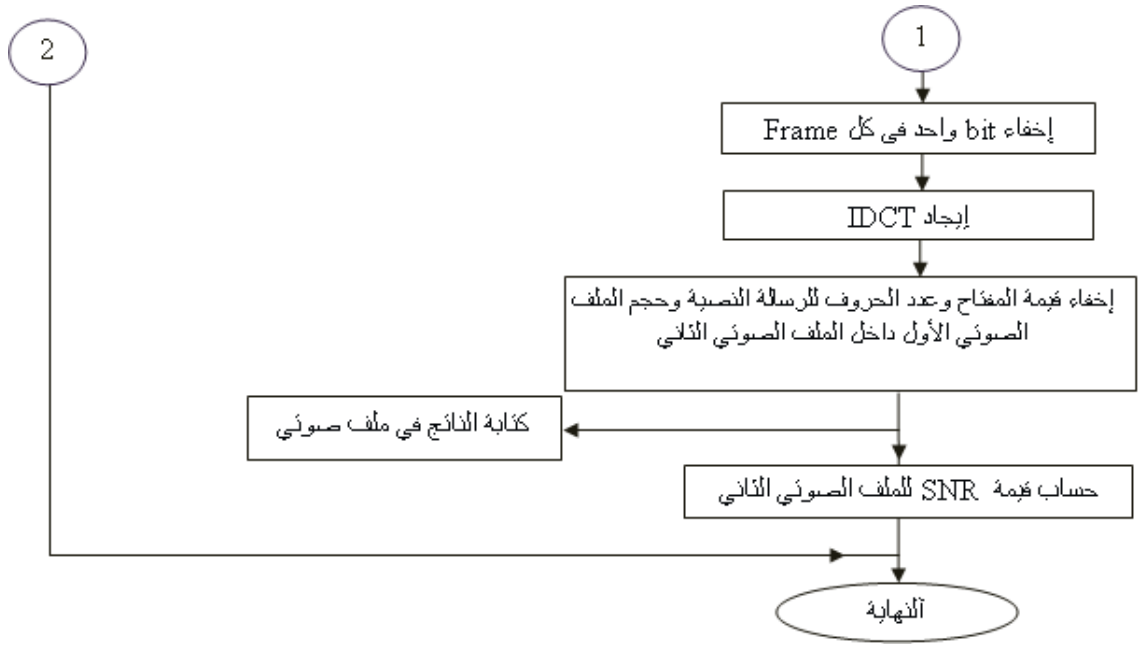
أما خوارزمية الاسترجاع فتتمثل باسترجاع النص بعد عملية فك الشفرة وبصورة صحيحة، إذ يتم استرجاع البيانات من مواقع متفق عليها من قبل الطرفين والمتمثلة بعدد الحروف وحجم ملف الصوتي الأول وقيمة المفتاح السري والتي عن طريقها يتم تحقيق الوثوقية للبيانات للتأكد من صحة الملف حيث يتم تقسيم الملف إلى مجموعة من الـframe بحجم (sample 8*1) وإيجاد الـ DCT لكل كتلة واسترجاع قيم البيانات التي تمثل الملف الصوتي الوسطي وقيمة المفتاح وحجم الرسالة النصية والملف الوسطي وعن طريق تحديد الموقع يتم استرجاع قيم الـbitsالتي تمثل الرسالة النصية وفك شفرة باستخدام المفتاح المسترجع، يتم استرجاع بيانات النص الأصلي.

1.3 خوارزمية الإخفاء المقترحة:

1- قراءة الرسالة النصية.
2- تشفير الرسالة باستخدام مفتاح متفق عليه وتحويلها إلى النظام الثنائي.
3- قراءة الملف الصوتي الأول وإيجاد طول الملف.
4- أ- إذا كان حجم الملف الصوتي أقل من عدد الـ bits للرسالة النصية أطبع الرسالة "لا يمكن استخدام الملف الصوتي الأول في إخفاء بيانات الرسالة المشفرة" أتجه إلى الخطوة (16).
ب- إذا الجواب (لا)، استمر...
5- إخفاء البيانات داخل الملف الصوتي في الخلية الأولى الأقل أهمية.
6- كتابة الناتج في ملف صوتي.
7- حساب قيمة SNR للملف.
8- قراءة الملف الصوتي الثاني وحساب طول الملف.
9- قراءة الملف الصوتي الأول وتحويل إلى النظام الثنائي.
10- أ- إذا كان الملف الصوتي الثاني أكبر من الملف الصوتي الأول الممثل بشكل ثنائي.
ب- إذا كان الجواب لا أطبع الرسالة "لا يمكن استخدام الملف الصوتي الثاني في إخفاء بيانات ملف الصوتي الأول اتجه إلى الخطوة (16).
11- تقسيم الملف الصوتي إلى مجموعة من الأطر وإيجاد DCT للملف الصوتي الثاني (حجم الـ Frame /Sample8)
12- إخفاء bit واحد في كل مقطع داخل الملف الثاني.
13- إيجاد IDCT.
14- إخفاء قيمة المفتاح وعدد الحروف للرسالة النصية وحجم الملف الصوتي الأول داخل الملف الصوتي الثاني.
15- حساب قيمة SNR للملف الثاني.
16- نهاية الخوارزمية

والشكل (1) يوضح المخطط الانسيابي لخوارزمية الإخفاء المقترحة.


البداية
إدخال الرسالة النصية
تشفير بيانات الرسالة باستخدام مفتاح معين
تحويل البيانات الناتجة إلى النظام الثنائي
قراءة الملف الصوتي الأول
حجم الملف >=عدد bit الرسالة النصية
لا
نعم
طباعة رسالة "لا يمكن استخدام الملف في إخفاء النص"
إخفاء البيانات داخل الملف الصوتي الأول في الخلية الأقل أهمية
كتابة الناتج في ملف صوتي
حساب قيمة الـSNR للملف
قراءة الملف الصوتي الثاني وحساب طول الملف
قراءة وتحويل الملف الصوتي الأول إلى مصفوفة أحادية
حجم ملف الصوت الثاني أكبر من الملف الأول
لا
طباعة رسالة "لا يمكن استخدام الملف الصوتي ألثاني في إخفاء الملف الصوتي الأول"
نعم
تقسيم الملف الصوتي إلى مجموعة من الأطر وإيجاد قيمة DCT للملف الصوتي الثاني
2
1



الشكل (1). المخطط الانسيابي لخوارزمية الإخفاء المقترحة

2.3 خوارزمية الاسترجاع المقترحة:

1- قراءة الملف الصوتي الثاني واسترجاع عدد الحروف للرسالة وقيمة المفتاح وحجم الملف الصوتي الأول في المواقع التي تم الاتفاق عليها من قبل الطرفين.

2- تقسيم الملف الصوتي إلى مجموعة من الأطر وإيجاد DCT للملف الصوتي.

3- استرجاع bit واحد من كل Frame وتحويلها إلى مصفوفة أحادية.

4- تكوين الملف الصوتي الأول بعد تحويل مجموعة bits إلى Samples.

5- حساب حجم الملف الصوتي الأول.

6- أ- إذا كان حجم الملف الصوتي الأول يساوي القيمة ألمسترجعة.

ب- إذا كان الجواب لا أطبع الرسالة "الملف المسترجع خاطئ" ثم اتجه إلى الخطوة (11).

7- استرجاع بيانات الرسالة النصية من الملف الصوتي.

8- إجراء عملية فك الشفرة بالاعتماد على قيمة المفتاح المسترجع.

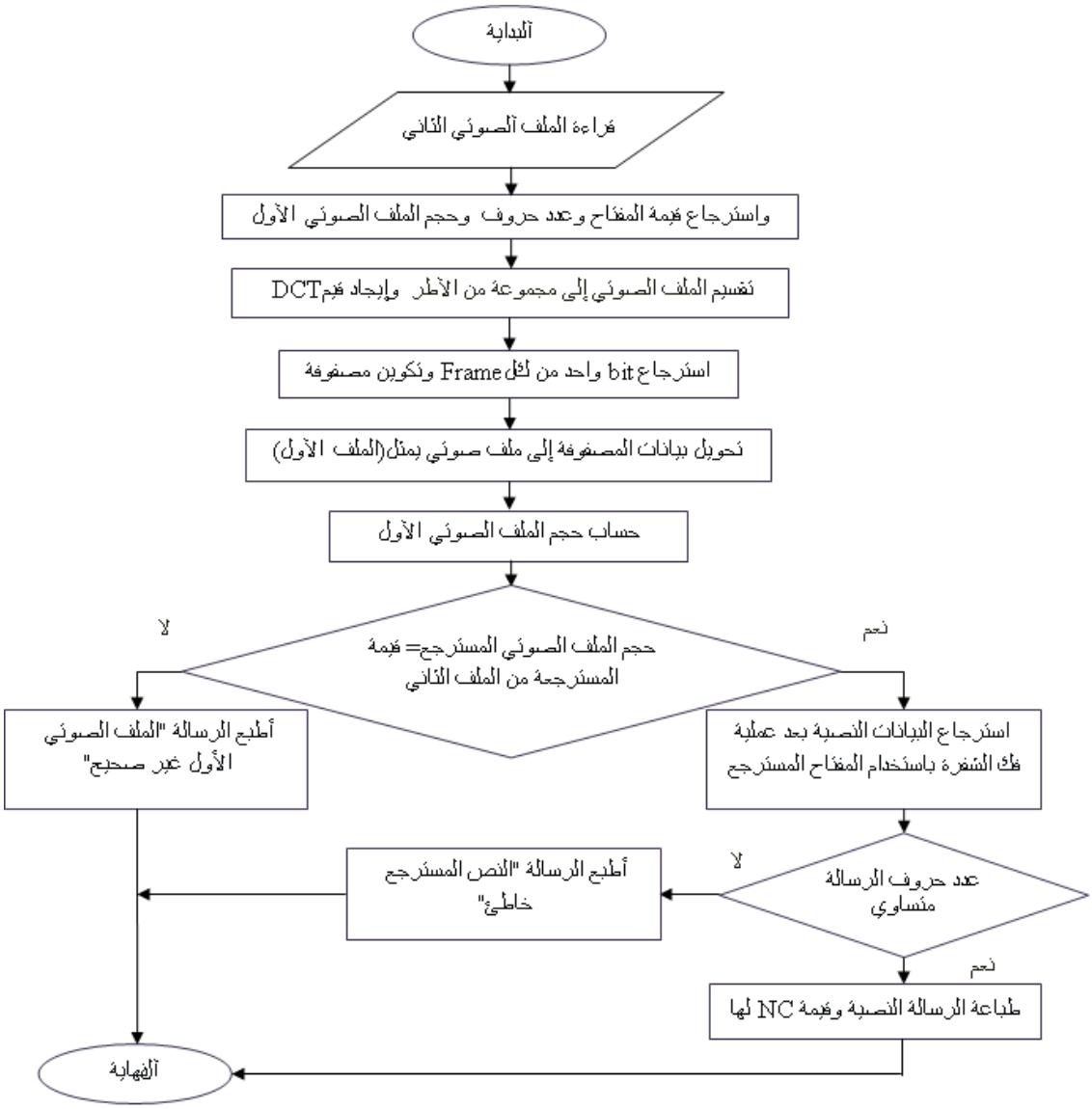
9- أ- إذا كانت عدد الحروف المسترجعة تساوي عدد الحروف المسترجعة من الملف الصوتي الثاني احسب قيمة NC للنص.

ب- إذا كان الجواب لا، أطبع الرسالة "الرسالة النصية خاطئة" اتجه إلى الخطوة(11).

10- طباعة الرسالة النصية وقيمة NC لها.

11- النهاية.

الشكل (2) يوضح المخطط ألانسيابي لعملية الاسترجاع



الشكل (2). المخطط الانسيابي لعملية الاسترجاع المقترحة

4. النتائج:

بعد تطبيق خطوات الخوارزمية الأولى والثانية تم استخدام المقاييس الآتية للتأكد من صحة البيانات المسترجعة وجودة الملفات الصوتية الحاوية على البيانات السرية:

1.4 معامل الارتباط التعياري Normalization Correlation (NC):

للتأكد من دقة البيانات المسترجعة تم اعتماد هذا المقياس والموضح في المعادلة (3)، كانت النتائج بالنسبة للصوت الأول وحروف الرسالة النصية تساوي واحد (NC=1).[1][9][6]

$$NC=\sum i \; sw(i) * s(i) / \sum i (s (i))^2 \quad \ldots(3)$$

2.4 مقياس نسبة الإشارة إلى الضوضاء Signal to Noise Ratio (SNR):

تم استخدام هذا المقياس للإشارة إلى عدم إدراك بيانات الرسالة السرية داخل الإشارة الأصلية وعدم ملاحظتها من قبل المستمع وكما في المعادلة الآتية[10][11][12]:

$$SNR = 10 * \log_{10} \frac{\sum_{n=0}^{N-1} X^2(n)}{\sum_{n=0}^{N-1} [X^{\circ}(n) - X(n)]^2}$$

حيث أن: X(n) تمثل الإشارة الأصلية. و $X^{\circ}(n)$ الإشارة الحاوية على العلامة المائية.

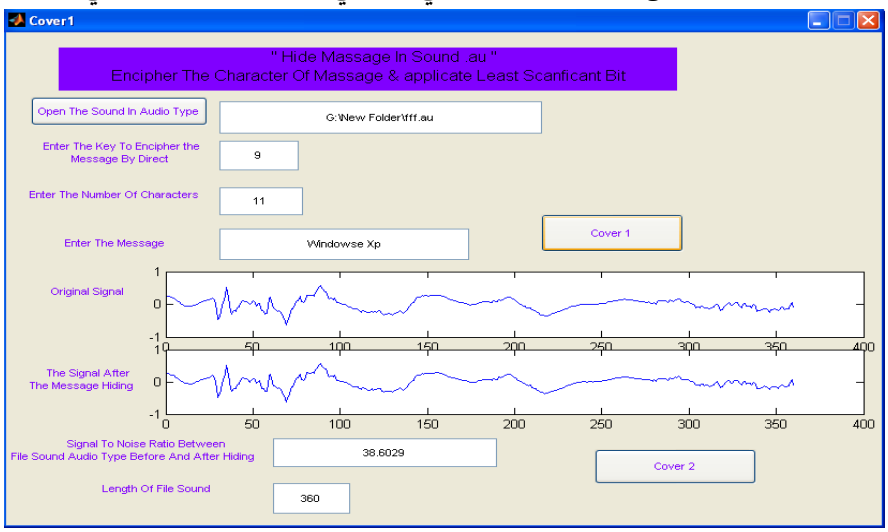
بعد تنفيذ الخوارزمية على عدة أنواع من ملفات الصوت، كانت قيمة معامل الارتباط التعياري NC=1 بالنسبة للرسالة النصية بعد عملية فك الشفرة والتأكد من حجم الملف الصوتي الوسطي والرسالة للتأكد من صحة الملف المضيف وقد كانت النتائج كما في الجدول التالي:

الجدول (1). يبين نتائج الخوارزمية

SNR للملف الصوتي المضيف	NC لحروف الرسالة	NC للصوت الوسطي	الرسالة النصية	الملف الصوتي المضيف	الملف الصوتي الوسطي
31.7136	1	1	University Of Mosul (19char)	paving.wav 392KB	ding.au 7.44KB
33.8847	1	1	Computer Science (16 char)	wav48.wav 840KB	ding.au 7.44KB
40.5666	1	1	hello world (11 char)	Fire_new.wav 192KB	ding.au 7.44KB

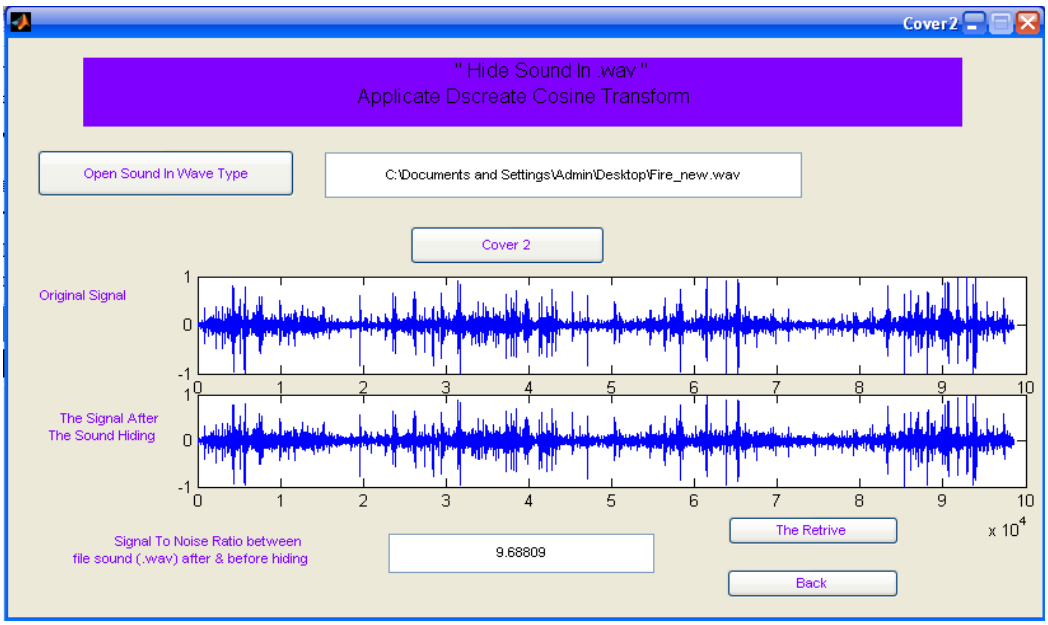
5. واجهات التطبيق:

تم الاعتماد في تطبيق الواجهات الرسومية من خلال لغة (Matlab) تحديدا من شاشة (Command) أو (M_file)، فالواجهة الأولى (الرئيسية) تضم فتح ملف صوتي من نوع (audio) وإدخال المفتاح لتشفير الرسالة بطريقة direct standard ويتم إدخال عدد حروف الـ message وإدخال ألـ message وعند النقر على الزر cover1 يختفي ألـ message المشفرة داخل الملف الصوتي الأول باستخدام (Least Significant Bit) وسيتم حساب قيمة Signal To Noise Ratio بين الملف الصوتي الأصلي والمضمن وكما مبين في الشكل رقم (3).



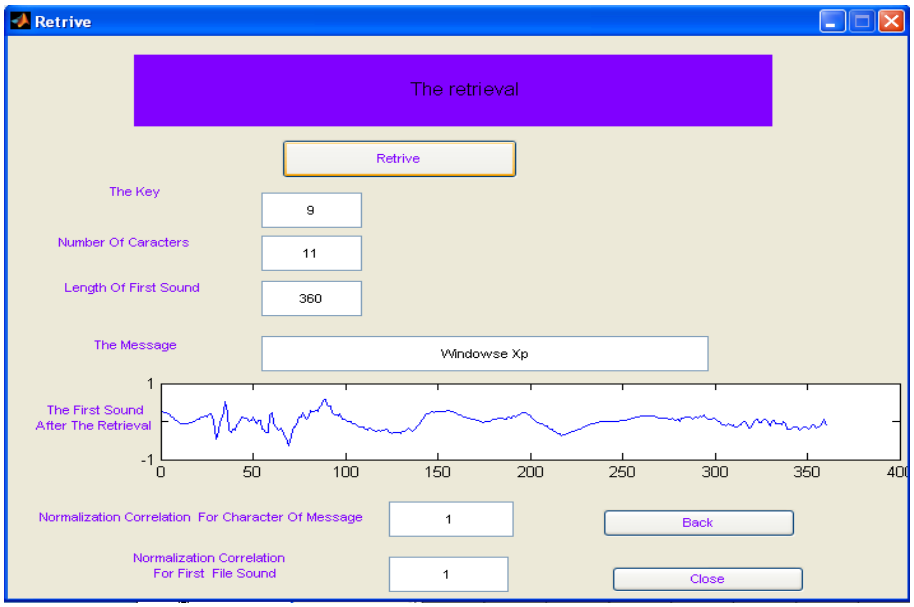
الشكل (3). الواجهة الرئيسية للتطبيق

وعند النقر على الزر Cover2 الموجود في الواجهة الأولى (الرئيسية) يتم فتح الواجهة الثانية المبينة في الشكل رقم (4) التي يتم فيها فتح الملف الصوتي الثاني (غطاء ثاني للملف الصوتي الأول) المخفي داخله ألـ message بطريقة (DCT) وسيتم حساب قيمة Signal To Noise Ratio بين الملف الصوتي الأصلي الثاني والمضمن.



الشكل (4). واجهة الإخفاء الثاني

وعند النقر على الزر retrievethe الموجود في الواجهة الثانية سوف ينتقل إلى الواجهة الثالثة (الاسترجاع) عند النقر على الزر Retrieve سوف يتم استرجاع ألـkey وعدد حروف ألـmessage وعدد ألـ samples وألـ message والملف الصوتي الأول وكما مبين في الشكل رقم (5).



الشكل (5). واجهة الاسترجاع

5. الاستنتاجات:

بعد تطبيق الخوارزمية المقدمة تم التوصل إلى الاستنتاجات التالية:

1- عملية تطبيق التشفير قبل إخفاء أي ملف أضافت سرية عالية للبيانات حيث لا يمكن الوصول إلى النص الصريح حتى لو حصل شك في وجود بيانات مخفية.

2- عملية الإخفاء أضافت قوة إلى أمنية البيانات المشفرة والتي تم التطبيق عليها.

3- بزيادة حجم ملف الصوت المضيف تبين أنه مهما كان حجم النص أو حجم الملف الصوتي الوسطي فإن النتائج تكون مرضية ولا يتم ظهور أي علامة أو شك في وجود بيانات.

4- بالرغم من صغر الملفات التي تم تطبيق الخوارزمية المقترحة عليها فان نتائج التطبيق حققت نجاح مرضي أمنيا، وباختبارها سمعياً لم يظهر أي تغيير على الملف المضيف.

6. الأعمال المستقبلية:

1- تنفيذ البنية المادية المعمارية لخوارزمية الإخفاء والاسترجاع على رقاقة الـ FPGA.

2- تنفيذ معمارية توازي للبنية المادية لجزء من الخوارزمية على رقاقة الـ FPGA.

3- تطبيق فكرة ألخوارزمية على أنواع أخرى من ملفات ألوسائط ألمتعددة.

المصادر

[1] الصميدعي، عامر تحسين سهيل، 2002، "تطبيق نظام التغطية"، بحث ماجستير، قسم علوم الحاسوب، كلية علوم الحاسوب والرياضيات، جامعة الموصل، العراق.

[2] Hong Doo Gun, Park Se Hyoung, Shin Jaeho, 2002, "A Public Key Audio Watermarking Using Patch work Algorithm", Department of Electronic Engineering, Dongguk University, Seoul, 100-715, Korea, proceedings of ITCCSCC.

[3] Jixin Lui, Zherning Lu, 2009, "A multipurpose audio watermarking algorithm based on vector quantization in DCT domain", world academy of science, engineering and technology pp618.

[4] Nidhi H Divecha, N N Jani, 2012, "Image Watermarking Algorithm using DCT, DWT and SVD", IJCA Proceedings on National Conference on Innovative Paradigms in Engineering and Technology (NCIPET 2012) ncipet(10):13-16, Published by Foundation of Computer Science, New York, USA.

[5] الحمامي، علاء حسين، محمد حسين، 2008، "إخفاء المعلومات الكتابة المخفية والعلامة المائية"، مكتبة جامعة الشارقة ص 29–84–102.

[6] http://en.wikipedia.org/wiki/Discrete_cosine_transform.

[7] R Sridevi, Dr. A Damodaram, Dr. Svl. Narasimham, 2009, "Efficient method of audio steganography by modified LSB algorithm and strong encryption key with enhanced security", Journal of Theoritical and applied information technology, Jntuh, Hyderabad.

[8] Al wahab Abed Adel, 2010, "Attack of multiplicative inverse without using extended Euclid's algorithm", Diyala Journal for pure sciences, vol. 6, no. 4., Dyala University College of education / AL-Razy Computer science department.

[9] Teruya Minamolo, Kenatro Aoki, 2010, "A blind Digital Image Watermarking Method using interval wavelet decomposition" International journal of signal processing, image processing and Pattern recognition, vol.3, no2, department of information science, Saga university, japan.

[10] داؤد، أكرم عبد الموجود، 2008، "استعادة الصور المشوهة والمضببة باعتماد طريقة التحويل المويجي"، بحث ماجستير، قسم هندسة الحاسوب، كلية الهندسة، جامعة الموصل، العراق.

[11] محمد، زهراء طارق، 2009، "تنفيذ البنية المادية لمرشح استخراج الحواف باستخدام FPGA"، بحث ماجستير، قسم هندسة الحاسوب، كلية الهندسة، جامعة الموصل، العراق.

[12] محمد، فرح طارق، 2004، "حماية استنساخ الكتابة باستخدام انتشار الطيف"، بحث ماجستير، قسم علوم الحاسوب، كلية علوم الحاسوب والرياضيات، جامعة الموصل، العراق.