الترقيم الدولي ٨٦٩٠ ـ ١٩٩١ ISSN 1991- 8690

Website: http://jsci.utq.edu.iq Email: utjsci@utq.edu.iq

# خوارزمية مقترحة لكشف التلاعب اوالتزوير في الرسائل والوثائق المرسلة عبر الشبكة

نجاة حميد قاسم

جامعة البصرة - كلية التربية - قسم علوم الحاسبات

## الخلاصةِ

يتضمن البحث خوارزمية مقترحة لكشف التلاعب اوالتزوير في الرسائل والوثائق المرسلة, حيث تمت برمجة هذه الخوارزمية بلغة فيجوال بيسك. تبنى هذه الخوارزمية من خلال إدخال رسالة نصية من قبل المستخدم التي استخرج منها مفتاح ( كلمة سر password ) واستخدم لتشفير معلومات عن صاحب الرسالة او الوثيقة ومن ثم الحاقها بتلك الرسالة لتمثل توقيع رقمي للرسالة او الوثيقة ومن ثم ارسالها .

تتلخص خوارزمية إيجاد المفتاح بالبحث عن الحروف التي تمثل منتصف كل كلمة بالرسالة ,ثم دمجها لتكوين المفتاح (بصمة الرسالة), تحول تلك الرموز إلى أرقام اسكى, ثم تجمع للحصول على رقم المفتاح الذي بدوره سيضاف إلى ارقام اسكي الخاصة بالمعلومات التي مثلت توقيع الرسالة, تحول الأرقام الناتجة إلى شفرة أسكي للحصول على التوقيع المشفر الملحق بالرسالة .عند استلام الرسالة يقوم المستلم باستخراج المفتاح (بنفس الطريقة اعلاه) لاستخدامه في فتح شفرة المعلومات, ان عملية فك الشفرة تكون معاكسة للعملية أعلاه , فاذا كانت الرسالة اوالوثيقة صحيحة يتم فتح الشفرة ومعرفة صاحبها ,اما اذا حدث تلاعب او تغيير في محتوى الرسالة فان المفتاح الناتج عند المستلم يكون مختلف عن المفتاح الاصلي عند المرسل وبهذا لايمكن فتح الشفرة وعندها تكون الرسالة مزورة .

## المقدمة

أدى التطور السريع والهائل في إمكانيات الحاسوب البرمجية والجهازية وظهور شبكة المعلومات العالمية إلى الحاجة للحفاظ على المعلومات عند تناقلها حيث ازداد الاهتمام بالمعلومات في الأعوام الأخيرة بشكل ملفت للنظر وأصبح حماية المعلومات من الأشخاص غير المخولين أمرا لابد منه وان إحدى الطرق المستخدمة لحماية المعلومات هي استخدام طرق التشفير.

إن الحاجة لتحسين امن البيانات والمعلومات في أنظمة الحاسبات الالكترونية هو نتيجة مباشرة للاستخدام المتزايد للحاسبات من قبل المصانع الحكومية والخاصة في معالجة وخزن وإيصال البيانات القيمة والحساسة وإضافة إلى ذلك فإننا نرى اهتماما حكوميا وعاما في مجال امن البيانات والمعلومات , كما ان المخاوف الأخيرة من جرائم الحاسبات والحاجة إلى

خصوصية المعلومات أدت أيضا إلى زيادة الاهتمام في التشفير ليكون وسيلة لإخفاء وحماية البيانات السرية ويمكن للتشفير ان يعطي درجة عالية من الأمن بأقل كلفة, وبما إن طرق التشفير التقليدية قد لا تعطينا الدرجة المطلوبة من الأمن, لذا قد تم تطوير تقنيات جديدة بحيث تعطي مستويات عالية من الأمن عند تطبيقها على نظام الحاسب هذه التقنيات الجديدة تستخدم مبادئ طرق التشفير التقليدية ومبادئ رياضية تطبق على الحاسب, كما استخدمت طرق الدمج بين التشفير والتوقيع الرقمي للحفاظ على خصوصية المعلومات المرسلة [2 ,1 ].

قبل البدء بالعمل نود التعرف على عملية التشفير وفك التشفيروكما يلي:

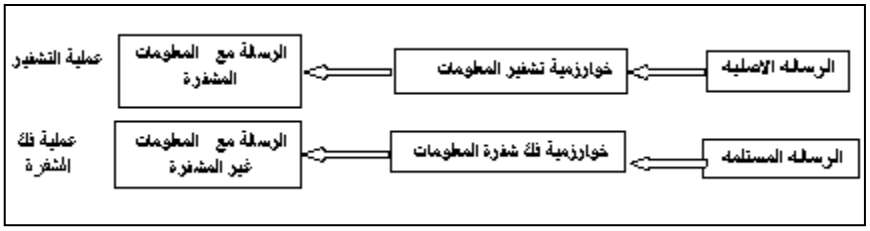
**التشفير وفك التشفير Encryption & Decryptions**

**١- مرحلة التشفير Encryption**

يعرف التشفير بأنه عملية تحويل المعلومات الى شفرات غير مفهومة (مشفرة), تم في هذه المرحلة تطبيق الخو ارزمية المقترحة لتشفير معلومات خاصة عن المرسل للحفاظ على خصوصية الرسالة .(شكل-١) يوضح عملية التشفير وفك الشفرة.

**٢- مرحلة فك الشفرة Decryptions**

هو تحويل المعلومات المشفرة إلى صيغتها الأصلية دون فقدان أو تشويه, تم في هذه المرحلة عكس خوارزمية تشفير المعلومات لإرجاعها الى وضعها الأصلي بأمان. [ 3 ,2] .




شكل (١) يوضح عملية التشفير وفك التشفير

**مفاتيح التشفير( Encryption keys )**

تستخدم المفاتيح في تشفير الرسالة وفك شفرتها وتستند هذه المفاتيح الى صيغ رياضية معقدة (خوارزميات) وتعتمد قوة وفعالية التشفير على عاملين الخوارزمية وطول المفتاح (مقدرا بالبت bit) هناك نوعين من أنظمة التشفير هما التشفير المتناظر والتشفير غير المتناظر, نظام التشفير المتناظر يستخدم نفس المفتاح في التشفير وفك الشفرة, أما النظام الغير متناظر يقوم بتوليد مفاتيح مختلفة ويستخدمها في التشفير وفك التشفير.في التشفير المتماثل يتم استعمال أساليب مبتكرة وصعبة لمنع الآخرين من اعتراض المفتاح واستخدامه في كسر الشفرة. في هذا البحث استخدم التشفير المتناظر اي استخدمت

خوارزمية لإيجاد المفتاح من اصل الرسالة التي يدخلها المرسل وبصورة متغيرة, لذا فان المفتاح يكون متغيرا وطوله يتغير ايضا"حسب الرسالة المدخلة وهذا نوع من الحماية والقوة المضافة للشفرة [ 3, 4 ].

## هدف البحث:

الهدف الاساسي لهذا البحث هو اكتشاف التلاعب او التزوير في الرسائل او الوثائق المرسلة عبر شبكة المعلومات حيث ان بعض الرسائل او الوثائق ترسل مفتوحة دون تشفيرها ' لذا تكون معرضة للتلاعب من قبل العابثين, كما في النشر الالكتروني والتجارة الالكترونية.

**مراحل تطبيق الخوارزمية المقترحة**

**a.** .ادخال الرسالة او الوثيقة المراد ارسالها, ثم ادخال معلومات عن صاحب الرسالة او الوثيقة.

**b.** تشفيرمعلومات صاحب الرسالة والحاقها باخر الرسالة.

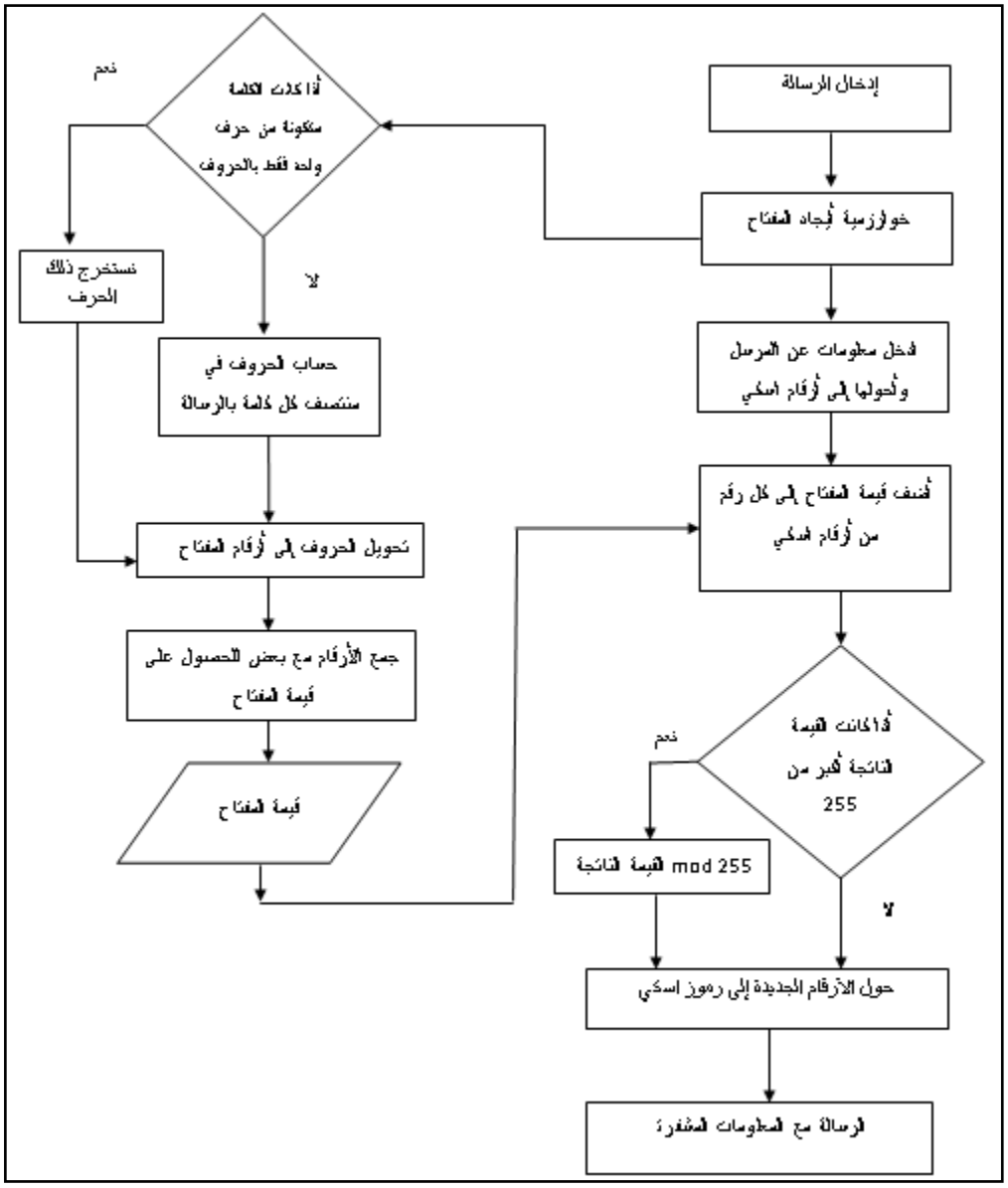
**c.** ارسال الرسالة وفتح شفرة المعلومات من قبل المستلم بعد استخراج المفتاح من نص الرسالة.

**الخوارزمية المقترحة لتشفير المعلومات Encryption Algorithm**

تتلخص خطوات الخوارزمية المقترحة بما يلي:

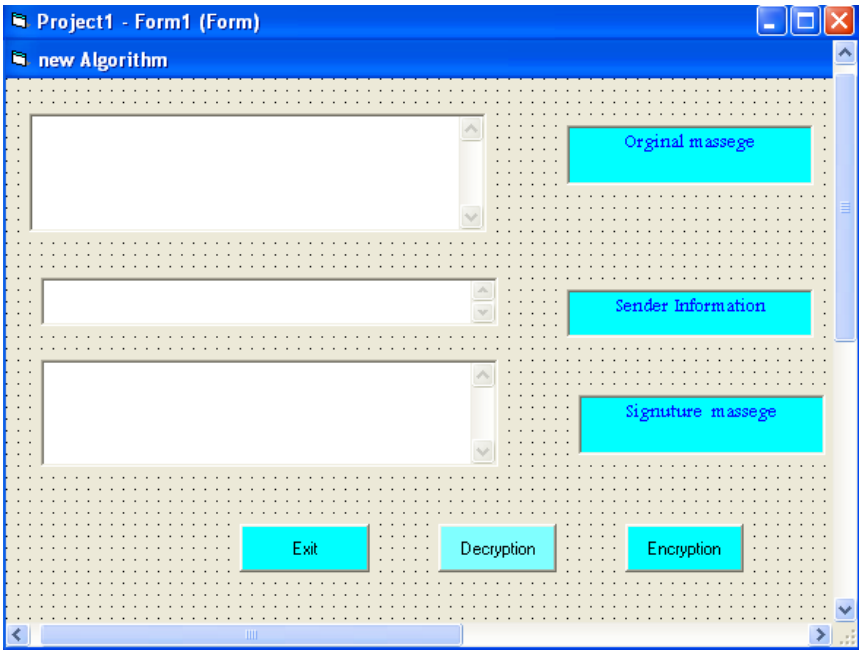
- إدخال معلومات عن المرسل او صاحب الوثيقة المراد ارسالها.
- إيجاد المفتاح او بصمة الرسالة بالبحث عن الحروف التي تكون في منتصف كل كلمة في الرسالة ثم دمج تلك الحروف معا لتكوين كلمة المفتاح, ( إذا كانت الكلمة متكونة من حرف واحد فقط يتم اخذ ذلك الحرف ).
- أحول حروف المفتاح إلى أرقام اسكي.
- اجمع أرقام المفتاح معا لأحصل على رقم المفتاح.
- أحول حروف المعلومات إلى أرقام أسكي.
- أضيف رقم المفتاح لكل رقم من أرقام تلك المعلومات لأحصل على أرقام جديدة , إذا كان الرقم الناتج اكبر من أخر رقم بالا سكي نأخذ له دالة mod لـ 255.
- أحول الأرقام الناتجة إلى رموز لأحصل على التوقيع المشفر.

الشكل( ٢ ) يوضح خطوات الخوارزمية.




شكل (٢) خوارزمية تشفير معلومات المرسل

وقد تم برمجة هذه الخوارزمية بلغة فيجوال بيسك vb وحسب النموذج الموضح بالشكل (٣). استخدم مربعا نص للإدخال احدهما لإدخال الرسالة والأخر لإدخال معلومات عن المرسل, واستخدم أيضا مربع نص أخر للإخراج لإظهار الرسالة الموقعة قبل وبعد الارسال, استخدم في البرنامج أيضا ثلاث كائنات أوامر commands الاولى تنفذ عملية التشفير للمعلومات والثانية تنفذ عملية فتح الشفرة والثالثة لإنهاء البرنامج.




شكل (٣) يوضح النموذج الذي تم تصميمه لتطبيق الخوارزمية

نقوم الآن باختبار البرنامج من خلال إدخال الرسالة التالية:

The digital audio- signal are analayzed based on MDCT(Modified-Discrete -Cosine Transform) to detect the masked coeffiecients of the spectrum. which are not transmitted in broadband networks. The algorithm interduce the most important concepts in audio compression and coding in MPEG systems.

شكل (٤-أ)-يمثل الرسالة الاصلية قبل التوقيع

ثم نقوم بادخال المعلومات التالية عن المرسل التي تمثل اسمه وعنوانه وتاريخ ووقت الارسال:

Najat Hameed-Basrah univercity-15/7/2009-04:15 PM

نلاحظ وحسب الخوارزمية إن الحروف التي تمثل المفتاح هي:

( Tgdgalaoiostttsiotchansiawtoetoociuradift)

إن حروف المفتاح أعلاه تم تحويلها إلى أرقام اسكى,ثم تجميعها معا لإنتاج رقم المفتاح المتمثل بالرقم (4342).

الجدول(١) يوضح الحروف التي تكون منها المفتاح مع شفرة اسكي المناظرة لكل منها دون تكرار, من الجدول يمكن ملاحظة ان الشفرة للحرف الكبير تكون مختلفة عنها لنفس الحرف الصغير

| قيم الحروف بالاسكي | حروف المفتاح |
|---|---|
| 84 | T |
| 103 | g |
| 100 | d |
| 97 | a |
| 108 | l |
| 111 | o |
| 105 | i |
| 115 | s |
| 116 | t |
| 99 | c |
| 104 | h |
| 110 | n |
| 119 | w |
| 101 | e |
| 117 | u |
| 114 | r |
| 80 | p |

ثم تجمع تلك الارقام معا للحصول على قيمة المفتاح النهائية وكما يلي:

Key=84+103+100+103+97+108+97+111+105+111+115+116+116+116+115+
105+111+116+99+104+97+110+115+105+97+119+84+111+101+116+111+
111+99+105+117+114+97+100+105+80+116 = 4342

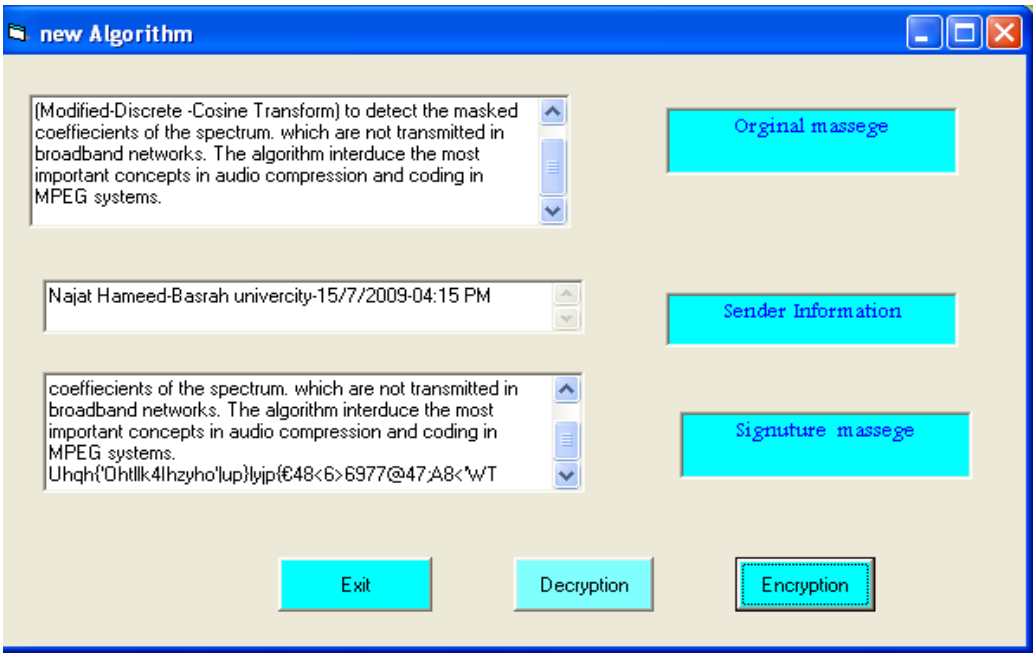
بهذه الطريقة تم توليد المفتاح الذي سوف نضيفه إلى كل حرف من حروف المعلومات بعد تحويلها إلى أرقام اسكي مما ينتج عنها أرقام جديدة[5,6] .

عملية الاضافة تلك سوف تزحف القيم الاصلية لشفرة المعلومات قبل تحويلها الى رموز اسكي وهذه العملية ادت الى حماية المعلومات من الوصول غير الشرعي اي (كسر الشفرة).حيث انه حتى ولو تم استرجاع القيم السابقة باي طريقة فانها لاتمثل القيم الحقيقية للمعلومات الا بعد طرح قيمة المفتاح من تلك القيم, وبما ان المفتاح غير معروف لانه يتم توليده بخوارزمية خاصة تكون معلومة فقط لدى المرسل والمستلم لذا فان اكتشافه يكون مستحيلا". اضافة الى انه يتغير باستمرار حسب تغير نص الرسالة او الوثيقة المرسلة مما يزيد من قوة الخوارزمية وفعاليتها الفريدة.

ان القيم الناتجة من عملية الاضافة السابقة تحول إلى رموز أو شفرات تمثل المعلومات المشفرة, ثم يتم الحاق تلك الشفرة بنص الرسالة المدخلة ليتم ارسالها, وكما في الشكل (٤–ب) يوضح تلك المعلومات بعد تشفيرها والحاقها بالرسالة الاصلية.

The digital audio- signal are analayzed based on MDCT(Modified-Discrete -Cosine Transform) to detect the masked coeffiecients of the spectrum. which are not transmitted in broadband networks. The algorithm interduce the most important concepts in audio compression and coding in MPEG systems.
Uhqh{'Ohtllk4Ihzyho'|up}lyjp{€48<6>6977@47;A8<'WT

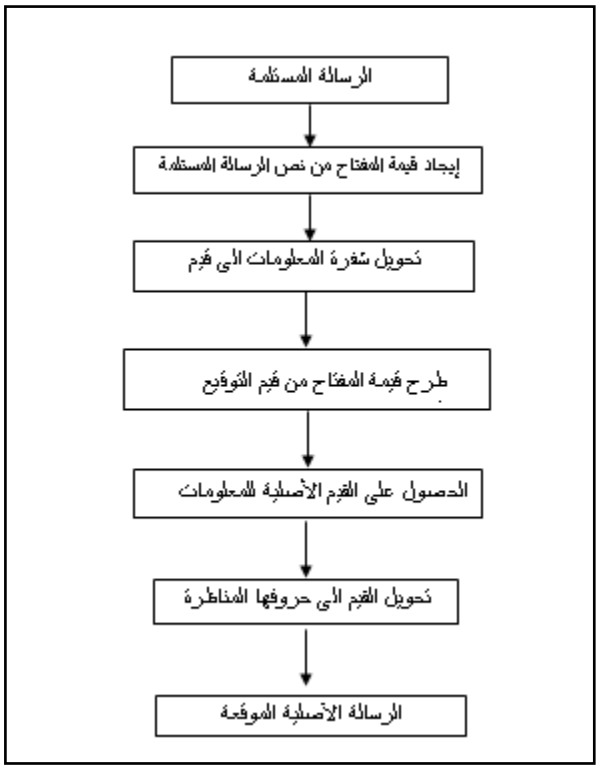
شكل (٤–ب) يمثل الرسالة الموقعة المرسلة




الشكل(٥) يوضح الرسالة المدخلة والرسالة المرسلة بعد تشفير التوقيع

**خوارزمية فتح شفرة معلومات المرسل: Decryption Algorithm**

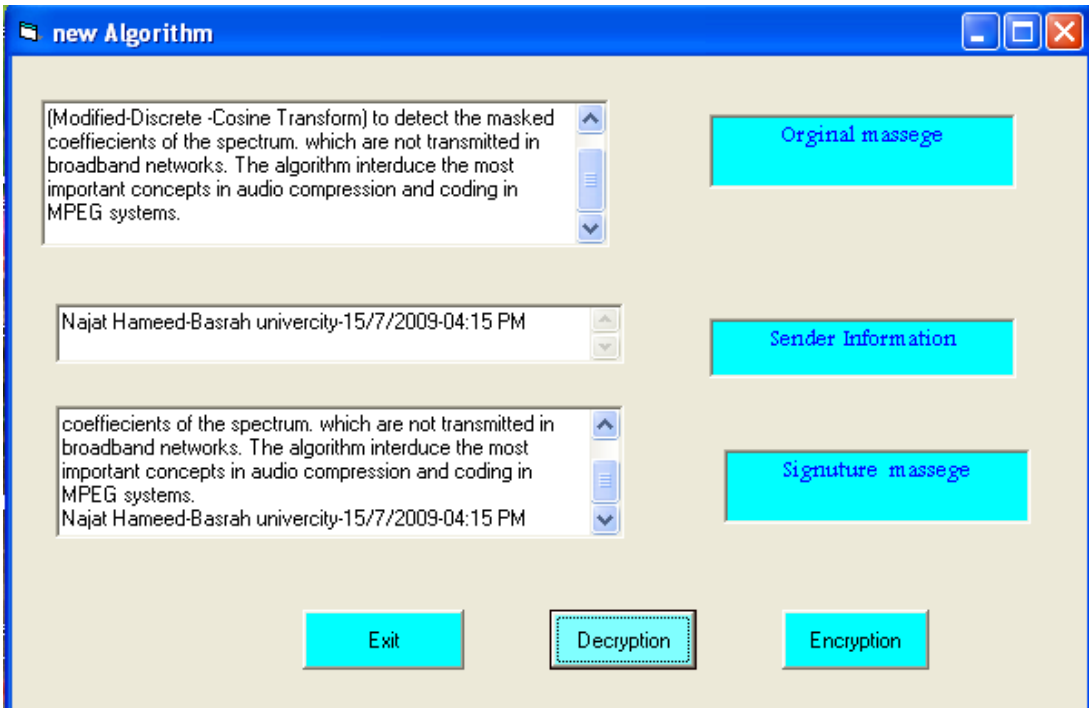
تعمل خوارزمية فتح شفرة المعلومات بصورة معاكسة لخوارزمية تشفيرها حيث عند استلام الرسالة الموقعة يتم فتح المعلومات المشفرة(توقيع الرسالة) من قبل المستلم حيث يقوم باستخراج المفتاح من نص الرسالة المستلمة (لانه المفتاح لايرسل مما يزيد من امنية المعلومات المرسلة),حيث انه يولد المفتاح بنفس الخوارزمية التي استخدمها المرسل. ومن ثم يتم عكس عملية التشفير من خلال طرح قيمة المفتاح من قيم رموز التوقيع للحصول على قيم الحروف الأصلية للتوقيع التي تمثل معلومات عن المرسل مثل ( اسمه وعنوانه وتاريخ ووقت الارسال), الشكل (٦) يوضح خطوات خوارزمية الفتح.




الشكل(٦) يوضح عملية فتح التوقيع المشفر

The digital audio- signal are analayzed based on MDCT(Modified-Discrete - Cosine Transform) to detect the masked coeffiecients of the spectrum. which are not transmitted in broadband networks. The algorithm interduce the most .important concepts in audio compression and coding in MPEG systems
Najat Hameed-Basrah univercity-15/7/2009-04:15 PM

شكل (٧) يمثل الرسالة المستلمة الموقعة بعد فتح شفرة التوقيع




الشكل(٨) يوضح الرسالة المدخلة والمستلمة بعد فتح شفرة التوقيع

ان كل ما ذكر اعلاه يتم على الرسالة الصحيحة اي لم يتم تغيير محتوى الرسالة من قبل العابثين فعند محاولة تغيير محتوى الرسالة المرسلة بعد توقيعها فمثلا حذف او اضافة كلمة او كلمات لتلك الرسالة فان المستلم لايستطيع فتح شفرة المعلومات لمعرفة المرسل لان المفتاح المتولد عند المستلم يكون مختلفا لاعتماده على نص الرسالة الجديد بعد التغيير وبذلك لايتطابق مفتاح المستلم مع المفتاح الاصلي للمرسل وبهذا تكون الرسالة مزورة.

فاذا تم تغيير الرسالة اعلاه وذلك بحذف كلمة (System) على سبيل المثال فان شفرة المعلومات لايمكن فتحها وكما في الشكل(٩).

كما تم تصحيح بعض الكلمات بالرسالة الاصلية الموقعة مثل ( analyzed, coefficients, introduce ) .

مما سبق يمكن ملاحظة ان التلاعب او التغيير بالرسالة يكون باضافة او حذف كلمة او كلمات ' كما ان بعض التصحيحات قد تسبب تغيير المفتاح .

The digital audio- signal are analyzed based on MDCT(Modified-Discrete -Cosine Transform) to detect the masked coefficients of the spectrum. which are not transmitted in broadband networks. The algorithm introduce the most important concepts in audio compression and coding in MPEG.
Uhqh{'Ohtllk4Ihzyho'|up}lyjp{€48<6>6977@47;A8<'WT

شكل (٩) يمثل الرسالة المزورة

## الاستنتاجات Conclusions

- بدا" سوف نناقش أهمية الخوارزمية من الناحية الأمنية, حيث كانت الرسالة المدخلة من قبل المرسل لها أهمية كبيرة من الناحية الأمنية بالنسبة للخوارزمية حيث أنها اعتمدت في بناء المفتاح الخاص الذي استخدم في تشفير معلومات المرسل , وبما إن الرسالة هنا متغيرة فان المفتاح سوف يتغير أيضا" بناءا" على ذلك لذا فان احتمالية كشف المفتاح تكون ضعيفة أو مستحيلة , إذن نستنتج بان هناك قوة في خوارزمية المفتاح كما ان طول المفتاح يزيد من صعوبة كشفه وكلما زاد طول الرسالة سوف تؤدي الى زيادة طول المفتاح اي ان المفتاح يكون متغير الطول كما تم توضيحه مما يزيد من قوة الخوارزميه .
- إن معلومات المرسل ممكن أن تكون رموز أو حروف أو أرقام.
- عند تغيير الرسالة المدخلة فان المفتاح سوف يتغير بناءا" على ذلك وعليه تتغير شفرة معلومات المرسل أيضا, لأنه بإضافة قيمة المفتاح الجديدة إلى أرقام رموز معلومات المرسل فسوف تنتج أرقام جديدة مما يؤدي إلى شفرة مختلفة.
- مما ذكر أعلاه نستنتج مرونة الخوارزمية في استقبال أي معلومات للمرسل لبناء المفتاح وبدون تقييد مما يزيد من قوة الخوارزمية وصعوبة الحصول على المفتاح شكل(٤-أ).
- عند جمع قيمة المفتاح مع قيم رموز المعلومات قد ينتج رقم يتجاوز أقصى رقم بالاسكي لذا تم استعمال دالة الـ mod لإرجاع الرقم ضمن أرقام رموز الاسكي, هذه العملية تم تجاوزها عند فتح المعلومات المشفرة وإرجاعها الى رموزها الأصلية.
- في هذه الخوارزمية لا يتم ارسال المفتاح الى المستلم او إعلامه عن قيمته وهنا تكمن قوة المفتاح بحيث لا يمكن الاعتراض له او كشفه, المستلم يولد المفتاح بناءا على الرسالة المستلمة وبنفس الخوارزمية التي استخدمها المرسل,ويقوم بفتح الشفرة للمعلومات فاذا لم تفتح الشفرة فهذا يعني ان الرسالة غير صحيحة.
- ان التغيير او التلاعب بالرسالة يكون بإضافة او حذف كلمة او كلمات من الرسالة المرسلة وبهذا سوف يتغير المفتاح بناءا على ذلك لذا لا تفتح شفرة المعلومات كما في الشكل(٩) .
- ان خوارزمية فتح المعلومات المشفرة كانت كفوءة جدا حيث أنها ترجع معلومات عن المرسل إلى أصلها وبصورة مطابقة وبدون زيادة أو فقدان للمعلومات كما في الشكل( 7).

## الاعمال المستقبلية future work

١. يمكن تطوير الخوارزمية باستخدام لغة فيجوال V.B.net

٢.يمكن تطويرالخوارزمية وذلك بتقليل حجم الرسالة من خلال اجراء خوارزمية ال hash عليها.

٣.يمكن تطوير خوارزمية المفتاح وذلك بضرب رقم المفتاح بعدد معين يمثل طوله.

## المصادر

٤- د.تاج الدين جرجس, د.عدنان معتزماوي, ٢٠٠٧," امان طرائق التواقيع الرقمية", مجلةجامعة تشرين للدراسات والبحوث العلمية-سلسلة العلوم الهندسية المجلد(٢٩) العدد(١).

٥- بروس بوزورت, ١٩٨٩, " الرموز الشفرات والحاسبات مقدمة الى امن المعلومات", الطبعة الاولى.
٦- الحمداني, وسيم عبد الأمير,١٩٩٢, "أنظمة التشفير", الطبعة الاولى.
٧- د.ابراهيم سليمان عبدالله," التجارة الالكترونية , أمن المعلومات-٢-", WWW.Kav.edu.sa/iabdullah.
٨. د.عبدالله مسفر الحيان/كليةالحقوق- د.حسن عبدالله عباس/كلية العلوم الادارية- جامعة الكويت, ٢٠٠٣ , " التوقيع الرقمي", مجلة العلوم الاقتصادية والادارية,المجلد (١٩), العدد الاول.
٩. مشرف ناصر الرويلي ,:كتاب طريق الاحتراف / الجزء الاول" – المملكة العربية السعودية , plantsman9009@hotmail.com.

1-Seberry J.& Pieprzyk J., 1989 "Cryptography An Introduction to computer Security", Prentice-Hall Incc>, U.S.A.
2-Denning D.E.R, "Cryptography and data security", Addison-Wesley Publishing company Inc., U.S.A., 1982.
3-Schneier B.,1996"Applied Cryptography Protocol, Algorithm and source code inc", john Wiley and sons, inc., U.S.A.

# An algorithm to discover any change with the messages or documents which is sent with the internet.

Najat H. Kassim

University of basrah - Collge of education - computer science

## Abstract

This research introduce new algorithm to discover any change in the sender message. This algorithm is programmed with visual Basic language. This algorithm is building from inputing message by the sender to find key or (password) for encoding the sender information , which is append to the original message and will be represents the message digital signature.

the algorithm of key will be search to find symbols that represents middle of any word ,this symbols will be concatenation to produced key in Ascii codes , which sum to produced key number that is added to each Ascii code from the sender information, as result ,every symbol is converted to Ascii code to produced new code append with message. the receiver will be produced key with the same algorithm above, then using it to decode message signature , by using the reverse algorithm of encoding , if this document or message is right, so the user information is read to know him .otherwise, the receiver will not decode this information so ,may be this document or message changed.