وثوقيـة ملف الصـوت

ياسين حكمت إسماعيل
قسم الحاسبات / كلية علوم الحاسوب والرياضيات
جامعة الموصل

إيمان فتحي احمد
قسم الحاسوب / كلية التربية
جامعة الموصل

الاستلام ١٨ / ٠٨ / ٢٠١٠
القبول ٠٥ / ٠١ / ٢٠١١

Abstract

Today the digital communication has become one of the most important things to the infrastructures in most applications, such as the Internet and in some cases which requiring confidential in communications that are confidential information become a sensitive issue. in this research we proposed a method to provide a way to achieve reliability in the digital audio files. Where we build a system to achieve the reliability of the digital audio through camouflage Uses one-way function and a summary of the message, as well as the idea of a digital signature.

Also we provide an efficient way to achieve the Digital Watermarking for digital audio. This research allows the recipient of the digital audio to ensure reliable voice and detect any possible change in the sound that occurs by any one during the sending over the computers network. We illustrate the results within the practical value of using the Matlab package ver. 7.0.

المستخلص

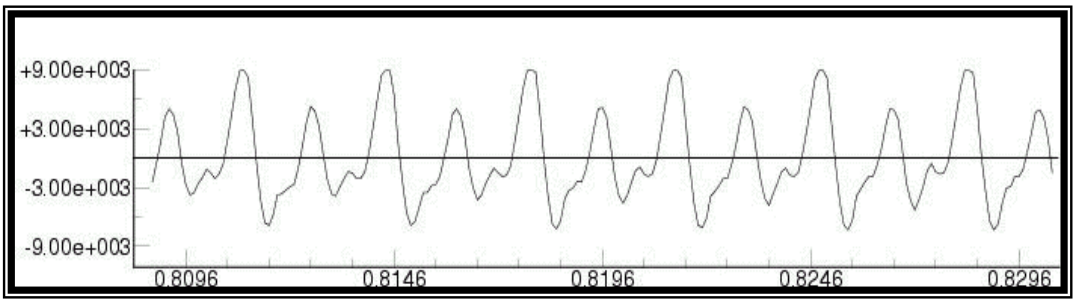
الاتصالات الرقمية أصبحت من الأمور المهمة للبنية التحتية اليوم في معظم التطبيقات مثل الانترنت وفي بعض الحالات التي تتطلب ان تكون الاتصالات سرية أي أصبحت السرية للمعلومات قضية أساسية، في هذا البحث تم تقديم طريقة مقترحة لتحقيق الوثوقية في ملفات الصوت الرقمية.

حيث تم بناء نظام لتحقيق الوثوقية للصوت الرقمي من خلال استخدام دالة التمويه أحادية الاتجاه لإخراج ملخص الرسالة ، كذلك فكرة التوقيع الرقمي . تم تقديم طريقة كفؤة لتحقيق

العلامات المائية (Digital Watermarking) للصوت الرقمي . هذا العمل يسمح لمستلم الصوت الرقمي التأكد م ن وثوقية الصوت والكشف عن أي تغيير في الصوت ممكن أن يحدث من قبل المتطفل أثناء إرساله عبر شبكة الحاسبات . تم توضيح النتائج ضمن الجانب العملي باستخدام لغة Matlab 7.0.

١. الصوت

يمكن تعريف الصوت على انه عبارة عن موجات ناتجة عن تغير في ضغط الهواء، وعلى الرغم من كون هذا التغير لا يتعدى (١±)، لكن عند ملامسته للأذن الداخلية فأنه يحرك طبلة الأذن ويُدرك كترددات صوتية مختلفة. يُمثل الصوت بمخطط على شكل خط متصل يُعرف بالموجة وارتفاع الموجة تمثل سعة الصوت (Volume) وهذه الصيغة تدعى بالإشارة التناظرية (Analog Signal) كما موضح في الشكل(١).



شكل (١): الإشارة التناظرية المستمرة

ينتقل الصوت في الوسط على شكل موجات (Waves)، إذ تحدث إزاحات في جزيئات الوسط بعيدة نسبيا عن مواقع التعادل، هذه الإزاحات تحدث تخلخل وتضاغط في جزيئات الوسط والذي بدوره يؤدي إلى انتقال الطاقة من مصدر الصوت الأصلي إلى جزيئات الوسط المجاورة لها، وهكذا بشكل دوري حتى تصل إلى جهة المستلم ويتطلب فهم الصوت معرفة المصطلحات الآتية:[7][3]

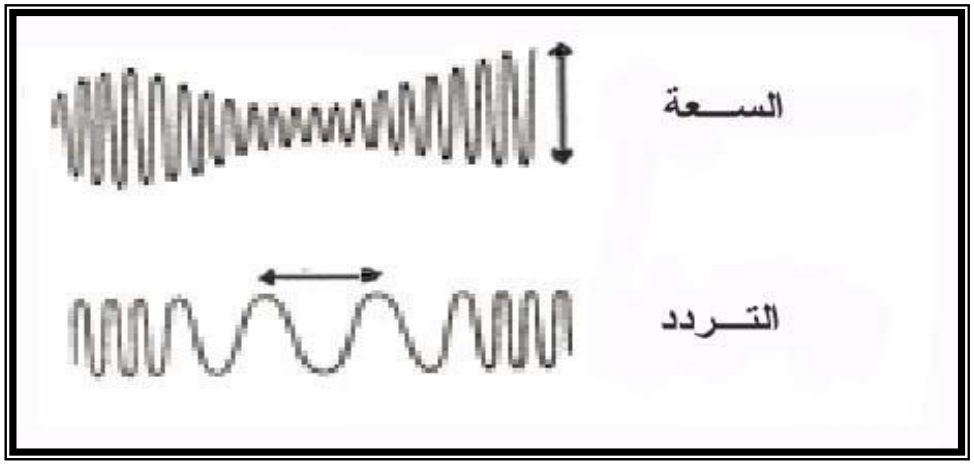
١.١ التردد (Frequency)

هو عدد المرات التي تغير بها الموجة طورها في الثانية الواحدة، ويقاس بالهيرتز (Hz: Hertz).

٢.١ سعة الموجة (Amplitude)

تسمى كمية التغيرات الحاصلة في ضغط الهواء نسبة إلى الضغط الجوي الطبيعي بـ (Amplitude) أو سعة الموجة وغالبا ما يستخدم هذا المصطلح للإشارة إلى قمة أو ذروة

الاتساع أي اكبر تغيير حاصل في ضغط الهواء والذي سبّبته موجة الصوت . وترتبط أيضا مع هذه الخاصية خاصية المحددة للصوت وهي الصخب (Loudness) ولكنها لا تطابقها تماما لان حساسية الإذن البشرية تختلف باختلاف التردد وان هذه الخاصية تعتمد على سعة الموجة وترددها، يبين الشكل (٢) الفرق بين تردد الموجة وسعتها. [٣] [٤] [7].



شكل(٢): الفرق بين التردد والسعة

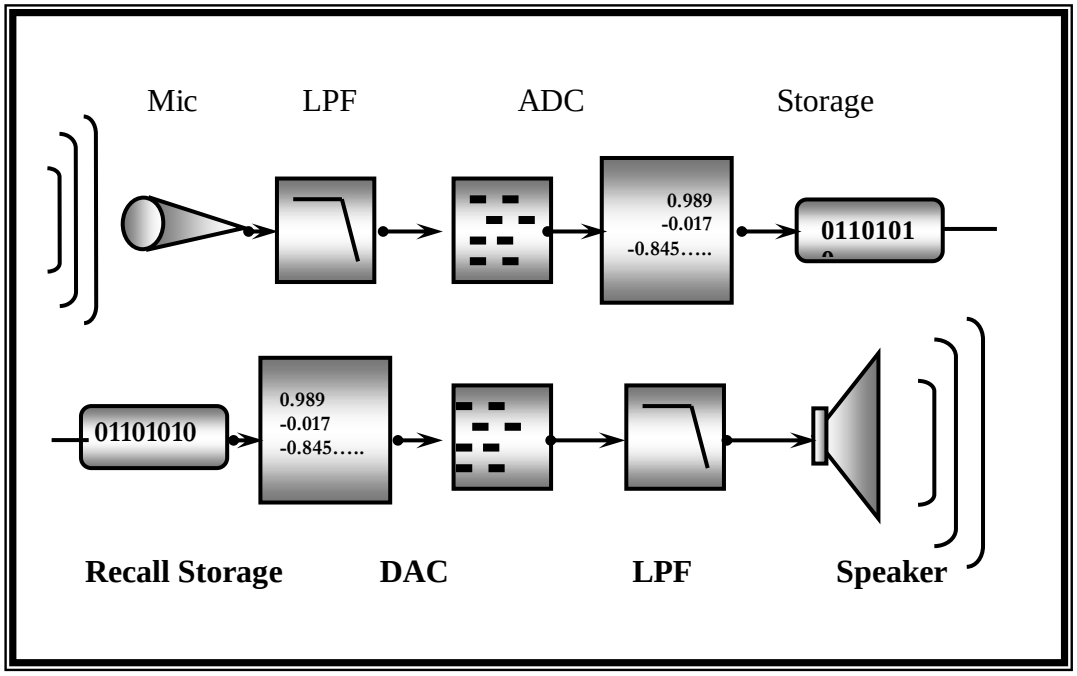
٢. الصوت الرقمي

الصوت عبارة عن إشارة تناظرية مستمرة (Continues Analog Signal) متواجدة في الأوساط التي تنتقل فيها سواء كان هذا الوسط هو الهواء أو أي وسط ناقل آخر .اما الحاسوب وبعض الأجهزة الكهربائية فإنها تتعامل مع الأشياء على أنها سلسلة من الأرقام الثنائية (1،0) أي بالصيغة الرقمية، ولهذا كان لابد من إيجاد وسيلة أو طريقة تحول الصوت من حالته التناظرية إلى الصيغة الرقمية (Digital Signal) لكي تستطيع هذه الأجهزة فهمه ومعالجته كما هو مطلوب[٤][15].

٣. تسجيل الصوت الرقمي

عند إدخال الصوت إلى الحاسوب من خلال لاقط صوت مربوط إلى بط اقة الصوت في الحاسوب فان لاقط الصوت (الميكرفون) يقوم بتحويل تذبذب ضغط الهواء إلى تذبذب في الفولتية على شكل إشارة تناظرية (Analog Signal) تعمل بطاقة الصوت عند استلام هذه الإشارة بقياسها وتحويلها إلى أجزاء تدعى بالعينة (Sample) ثم يتم تحويلها إلى سلسلة من الأرقام بعملية تدعى التكميم (Quantization) ومن ثم يتم تحويلها إلى صيغة ثنائية، وتخزن هذه العينات داخل الحاسوب على الذاكرة الثانوية (القرص الصلب) بصيغة رقمية ثنائية . يساعد في هذه العمليات دائرة إلكترونية موجودة على بطاقة الصوت تدعى ADC (Analog to

Digital Converter). عند إعادة تشغيل الصوت (Play Back) يتم عكس العملية إلا أن التذبذب في الفولتية سوف ينتقل إلى مكبرات الصوت بدلا من لاقط الصوت ثم يحول إلى تذبذب في ضغط الهواء . وهناك أيضا دائرة إلكترونية تعمل على إعادة الصوت إلى حالته التناظرية مرة أخرى تدعى DAC ، والشكل (٣) يوضح هذه العمليات[12]:



شكل(٣): تحويل الصوت من الصيغة التناظرية إلى الصيغة الرقمية والعكس

هناك عوامل تأثر على عملية تسجيل الصوت الرقمي (Digital Sound) منها:

أولاً: عدد قنوات التسجيل (Number of Channels):

عند تسجيل الكلام باستخدام الأسلوب ا لأحادي (Mono) يتم اعتماد لاقط صوت واحد لالتقاط الصوت ثم تحويله إلى إشارة رقمية . أما عند استخدام الأسلوب المجسم (Stereo) في التسجيل فيتم اعتماد اكثر من لاقط صوت واحد لغرض التقاط الصوت وهذا يعتمد بشكل مباشر على بطاقات الصوت التي تعمل على التسجيل ضمن النظام ا لمجسم، أي يتم تسجيل عينة للميكرفون الأيسر ثم عينة للميكرفون الأيمن، وبالتالي فان حجم الملف الصوتي المستخدم ضمن النظام المجسم يكون ضعف الملف المسجل ضمن النظام الأحادي (Mono) [2].

ثانياً: معدل التعيان (Sampling Rate)

الملفات الصوتية الرقمية تخزن المعلومات على شكل سلسلة طويلة من العينات الصوتية وعملية التعيان هي الفترة الزمنية المختارة لتمثيل العينة الصوتية عند تحويلها من الصيغة

التناظرية (Analog Signal) إلى الصيغة الرقمية (Digital Signal) وكلما زاد عدد العينات المأخوذة في الثانية الواحدة زادت دقة وجودة الصوت المخزون وهذا يعني زيادة (Sampling Rate) وبالتالي زيادة حجم الملف الصوتي [1].

ثالثاً: تكميم العينة (Quantization)

وتعرف أيضاً بالوضوحية (Bit Resolution) و يقصد به عدد الوحدات الخزنية (Bits) المستخدمة لتمثيل عينة الكلام وهي من العوامل المهمة أيضاً في المح افظة على دقة الصوت عند تسجيله بالأسلوب الرقمي إذ يكون الصوت ذو مواصفات قريبة جدا من الإشارة المستلمة كلما زاد عدد الوحدات الخزنية المستخدمة لغرض تمثيل العينة . إن أقل بطاقة للصوت توفر تكميم للعينة (8bit)، إلا إن التكميم بـ (16bit) يعد مناسباً في أغلب الحالات [12][4].

٤. ملفات خزن الصوت

قبل الولوج في الحديث عن موضوع الملفات الصوتية وصيغ خزنها، لابد من معرفة المقصود بمصطلح صيغة خزن الملف (File Format). صيغة خزن الملف هي طريقة خاصة لترميز البيانات (Data) تستخدم لغرض خزن البيانات في ملف داخل الحاسوب، وأما الملف الذي يتم فيه خزن البيانات الصوتية داخل الحاسوب فيدعى بـ (Sound File Format). هناك العديد من صيغ خزن الملفات الصوتية، يتميز كل نوع بخاصية معينة ينفرد بها عن غيره من الملفات منها (AU, WMA, MP3, WAV) [6].

١.٤ ملفات الـ (wav)

لأن الـ wave هي من صيغ الصوت ال مستخدمة بشكل عادي في (Microsoft Window) بيئة نظام الـ Window لذا فهي تعتبر من أحد صيغ الصوت الشائعة حالياً الـ Microsoft تعرف هيئة الملف (format) العامة (RIFF) Resource Interchange file format.ملفات الـ RIFF نظمت كمقاطع متداخلة ومترابطة مع بعضها التي تتضمن تعريف لمحتويات الـ RIFF.

٢.٤ تحليل الـ Header لملف الـ wave.

ملف wave الذي هو نوع خاص من ملف ال RIFF الذي يحتوي على مقاطع متداخلة ومترابطة كل مقطع يتكون من اربع رموز (مثل RIFF، fmt، list، disp 1، Data) ثم تتبع

بـ (byte-4) تشير الى حجم البيانات التي يتضمنها المقطع . الأنواع الخاصة من المقاطع مثل (RIFF و List) فإنها تتضمن مقاطع أخرى . الجدول (1) يبين أحد أنواع صيغ مقاطع الـ RIFF والتي تتضمن المقاطع الأخرى[3].

الجدول (1): محتويات المقطع RIFF

Size Information In byte	Offset	Contains	Description
4	0	"RIFF"	Signature for resource interchange file format
4	4	size	Total file size- 8
4	8	"WAVE"	Signature for audio RIFF file
4	12	"fmt ∇ "	After it information about the sound
4	16	16/18	Size of info after this location
2	20	Compression code	Usually 1=PCM:0 not compressed
2	22	Number of channels	1 mono, 2 stereo
4	24	Samples per second	The sampling rate of the file
4	28	Bytes per second	Number of bytes per second
2	32	Sample size in bytes	Size of sample in bytes
2	34	Sample size in bits	Size of sample in bits
2	36	Reserved	This location is exist if offset 16 contain 18
4	36/38	"data"	Chunk type data
4	40/42	Length of sound data	The length of the sound data in bytes
Length of data	N	Signal	Actual sound samples

٦. الوثوقية (Authentication).

أن مفهوم الوثوقية هو التأكد من أن الاتصال بين الحاسبات (Computer Communication) موثوق به . هنالك نوعين من الوثوقية وهي وثوقية المستخدم ووثوقية الرسالة . تتضمن وثوقية المستخدم قابلية تحديد مستلم الرسالة (البيانات) من تحديد مدى وثوقية الجهة المرسلة ، في حين أن وثوقية الرسالة تتضمن قابلية المستلم من تحديد وثوقية البيانات المرسلة أي التأكد من سلامة البيانات وأنها لم تتعرض لأي تغيير أثناء أنتقالها عبر شبكة الحاسبات. [8][14] [5].

٧. ملخص الرسالة (Message Digest).

عملية تمثيل الرسالة بسلس لة مفردة من الأرقام تسمى بالبصمة الإلكترونية للرسالة (Message Digest)، وعملية تشفير البصمة الإلكترونية للرسالة باستخدام أنظمة التشفير اللامتماثل يولد توقيعاً رقمياً للرسالة، والذي يعد المعنى الإلكتروني للوثوقية . ممكن أن تستخدم التواقيع الرقمية لتوثيق هوية المرسل للرسالة أو الموقع للوثيقة ، وكذلك تستخدم التواقيع الرقمية للتأكد من أن محتويات الرسالة أو الوثيقة والتي تم نقلها (إرسالها) لم تتغير ، على الرغم من أن التشفير يمنع المتلصِّصين من الاطلاع على محتويات الرسالة ، إلا أنه لا يمنع المخرِّبين من العبث بها؛ أي أن التشفير لا يضمن سلامة الرسالة (Integrity)[16].

٨. دوالّ أو إقترانات التمويه (hash functions).

تم استخدام دوال التمويه في مجال علوم الحاسبات لمدة طويلة ، حيث إن دالة التمويه هي دالة رياضية إدخالها عبارة عن سلسلة من البيانات ذات طول متغير تعرف ب الصورة الأصلية (Pre-Image) والتي تمثل الرسالة أو البيانات المراد إيجاد قيمة دالة التمويه لها حيث تقوم دالة التمويه بتحويل الطول المتغير (العشوائي) للبيانات المدخلة إلى سلسلة من البيانات ذات طول ثابت (Fixed Length) والتي عادة يكون طولها اص غر من طول البيانات المدخلة. وقد تكون دالة التمويه عبارة عن دالة تقوم باستلام البيانات ذات الطول المتغير وتقوم بإرجاع بايت (Byte) واحد والناتج من إجراء عملية (XOR) لجميع بايتات (Bytes) الإدخال. والهدف من دالة التمويه هو تكوين بصمة (سلسلة من البيانات) للبيانات المدخلة حيث إن قيمة البصمة تساعدنا على التحقق من أن رسالتين معينتين تكونان متساويتان إذا كان لهما قيمة دالة التمويه نفسها (البصمة نفسها)[13] .

٩. دالة التمويه أحادية الاتجاه (One Way Hash Function).

هي دالة رياضية إدخالها عبارة عن سلسلة من البيانات ذ ات طول متغير ، حيث تقوم دالة التمويه بتحويل الطول المتغير (العشوائي) للبيانات المدخلة إلى سلسلة من البيانات ذات طول ثابت (Fixed Length) والتي عادة يكون طولها أصغر من طول البيانات المدخلة . دالة التمويه أحادية الاتجاه هي الدالة التي تعمل باتجاه واحد فقط فمن ا لسهولة حساب قيمة التمويه (Hash Value) للبيانات المدخلة ولكن من غير الممكن الحصول على البيانات الأصلية، أي أذا تم الحصول على قيمة التمويه فمن الصعوبة الحصول على البيانات الأصلية التي أشتقت منها تلك القيمة. [13] [9] [16]

١٠. التوقيع الرقمي (Digital Signature).

هو عبارة عن مقطع من البيانات ناتج من تشفير ملخص الرسالة باستخدام المفتاح السري (المفتاح الخاص) للمرسل. يتم إضافة التوقيع الرقمي إلى الرسالة لأثبات هوية مرسلها وضمان سلامة محتوياتها أثناء أرسالها عبر قناة النقل (Transmission Channel) ضمن شبكة الحاسبات.[5][16]

١١. العلامات المائية الرقمية (Digital Watermarking)

أصبحت العلامة المائية تقنية مختارة لمدى واسع من تطبيقات حماية حقوق الوسائط المتعددة. و قد تم استخدامها لتضمين بيانات مستقلة التشكيل في إشارات صوتية/فيديوية بطريقة قوية للتحرير وهي احدى تقنيات اخفاء المعلومات (Information Hiding Technique) تستخدم لاثبات الملكية (Intellectual Property) او لضمان الوثوقية. الية العلامات المائية الرقمية تتضمن اخفاء بيانات قلي لة نسبيا ضمن بيانات اخرى (كوسط ناقل)، أي لدينا بيانات والمراد طمرها داخل وسائط اخرى (ملفات نصية، صورية وصوتية). هنالك العديد من الأمثلة عن استخدام تقنية العلامات المائية منها معلومات حق الاستنساخ (Copyright Information)، توقيع المؤلفين الرقمي (Digital Authors Signature) وتوثيق الشركة (Company Logo) وكلها وسائل تمثل شرعية المالك [9][2].

١٢. الجانب العملي.

يتضمن الخوارزمية المقترحة وهي كما يلي:

١.١٢. الخوارزمية المقترحة.

يتم توضيح فكرة الخوارزمية المقترحة من خلال خوارزميتي الجهة المرسلة والمستلمة:

أولاً: خوارزمية الجهة المرسلة وتتضمن إجراء الخطوات التالية:

أ- قراءة ملف الصوت نوع WAV وتحويلهَ ُ ُ ُ إلى مصفوفة.

ب- يتم تحويل المصفوفة ذات الابعاد (2 * i) الى مصفوفة ذات الإبعاد (4 *i).

ج- حساب قيمة الـ Message Digest من خلال أجراء عملية XOR لصفوف المصفوفة الناتجة من الخطوة ب والحصول على ثلاثة قيم لـ Message Digest حيث أن:

١. القيمة الاولى تتضمن عملية الـ XOR لصفوف المصفوفة من البداية وحتى المنتصف.

٢. القيمة الثانية تتضمن عملية الـ XOR لصفوف المصفوفة من المنتصف وحتى النهاية.

٣. القيمة الثالثة تتضمن عملية الـ XOR لجميع صفوف المصفوفة مع أسم الملف الصوتي.

د- إضافة قيم الـ Message Digest الثلاثة التي تم حسابه ا في بداية ووسط ونهاية المصفوفة، وهي تمثل اسلوب جديد لتحقيق تقنية العلامات المائية.

هـ- إجراء عملية التشفير للمصفوفة باستخدام طريقة الـ Column Transposition الإبدال العمودي باستخدام مفتاح معين.

و- إرجاع المصفوفة (i*4) الى مصفوفة (i*2) والحصول على ملف الصوت المشفر.

ثانياً: خوارزمية الجهة المستلمة وتتضمن إجراء الخطوات التالية:

أ- يتم قراءة ملف الصوت والمشفر وتحويله إلى مصفوفة.

ب- يتم تحويل المصفوفة ذات الأبعاد (i*2) إلى مصفوفة ذات الأبعاد (i*4).

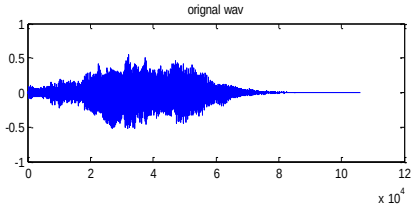
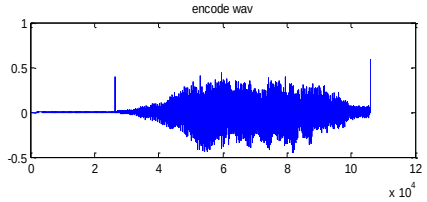
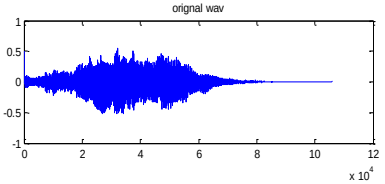
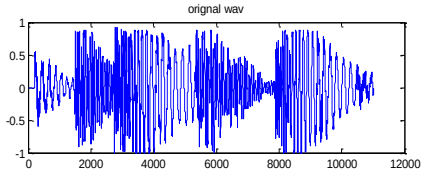
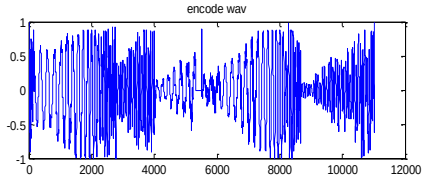
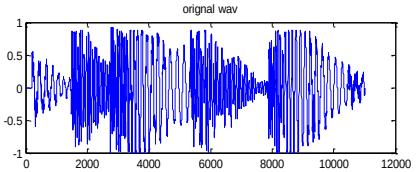
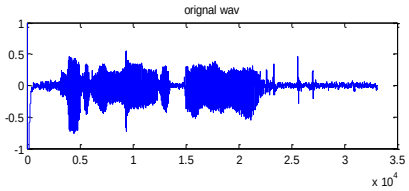
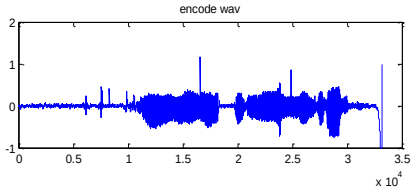
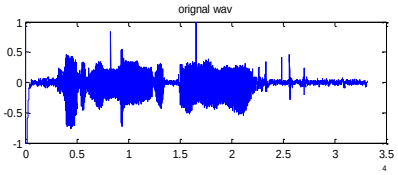
ج- سحب قيم الـ Message Digest من بداية ووسط ونهاية المصفوفة . والحصول على مصفوفة ناتجة جديدة.

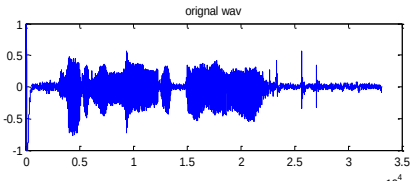
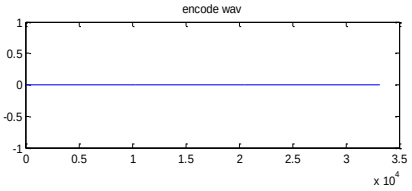
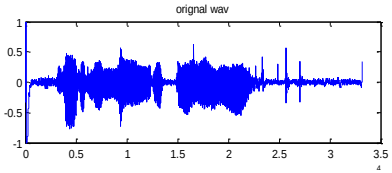
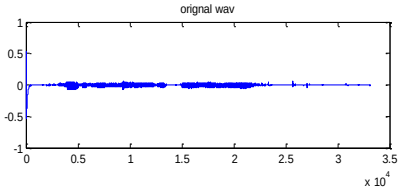
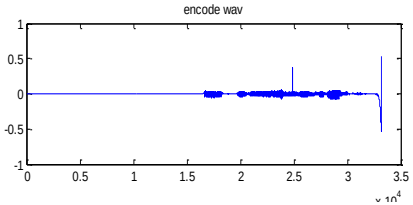
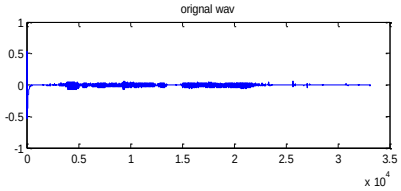
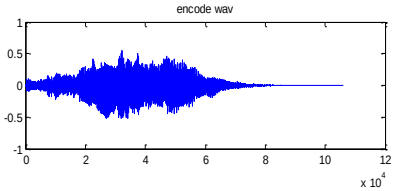
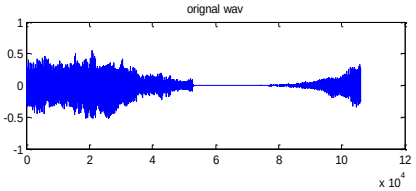
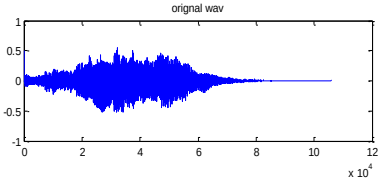
د- حساب قيم الـ Message Digest للمصفوفة الناتجة من الخطوة ج وبنفس الأسلوب المستخدم في خوارزمية الجهة المرسلة.

هـ- مقارنة قيم الـ Message Digest المحسوبة مع المستلمة فأذا تطابقت القيم دل ذلك على أن ملف الصوت المستلم موثوق به ، واذا لم تتطابق القيم دل ذلك على أن الملف غير موثوق به، علماً بأن عملية التطابق تتضمن نسبة خطأ قليلة نسبياً تقريباً 0.0001.

١٣. مناقشة النتائج

تم تطبيق عملية التشفير وفك التشفير على عدد من العينات الصوتية عن طريق الإبدال العمودي للأعمدة باستخدام مفـتاح معين حيث كانت النتائج كما موضح في الجدول (١).

Original Wav (1)	Size	Encode Wav(1)	Size	Original Wav (1)	Size
	١٠٦١٥٠		١٠٦١٥٦		١٠٦١٥٦
Original Wav (2)	Size	Encode Wav(2)	Size	Original Wav (2)	Size
	11025		11032		11032
Original Wav (٣)	Size	Encode Wav(٣)	Size	Original Wav (٣)	Size
	33215		33222		33222

Original Wav (4)	Size	Encode Wav(4)	Size	Original Wav (4)	Size
	33215		33222		33222
Original Wav (5)	Size	Encode Wav(5)	Size	Original Wav (5)	Size
	33215		33222		33222
Original Wav (6)	Size	Encode Wav(6)	Size	Original Wav (6)	Size
	106150		106156		١٠٦١٥٦

يتبين من الحالات السابقة أن عملية التشفير عن طريق الإبدال العمودي Column Transposition لمصفوفة الملف ا لصوتي كانت كفوءة بحيث أن الملف الناتج يختلف بشكل كبير عن الملف الاصلي.

١٣. الاستنتاجات

نستنتج من هذا البحث

١. أمكانية تحقيق الوثوقية باستخدام تقنية العلامات المائية الرقمية (Digital Watermarking) وتم ذلك من خلال إضافة قيم Message Digest في بداية ووسط ونهاية مصفوفة ملف الصوت.

٢. استخدام طريقة تقليدية في التشفير (طريقة الإبدال العمودي Column Transposition) وهي من الطرق السهلة والسريعة التطبيق ، حققت نتائج جيدة عند استخدامها مع الملفات الصوتية.

٣. تم اكتشاف حالات التغيير التي تحدث على الملف الصوتي وبصورة كفوءة ، فكما هو معروف أن تغيير بت واحد أو عدد قليل من البتات في مصفوفة الملف الصوتي لا تؤدي إلى تغيير ملحوظ في الصوت المتحسس من قبل الأذن البشرية، تبين ذلك من خلال تغير ملحوظ على طول ملف الصوت.

١٤. المصادر:

١) الجوهري، شيماء شكيب محمد ، (٢٠٠٤)، "الاخفاء في ملف صوت مك بوس"، بحث ماجستير، كلية علوم الحاسبات والرياضيات، جامعة الموصل، العراق .

٢) الصميدعي عامر تحسين سهيل ، (2002)، "تطبيق نظام التغطية"، بحث ماجستير ، كلية علوم الحاسبات والرياضيات، جامعة الموصل، العراق.

٣) عبد القادر، إسراء عبد السلام ، (٢٠٠١)، "كبس الصوت عند الزمن ا لحقيقي"، بحث ماجستير، كلية علوم الحاسبات والرياضيات، جامعة الموصل، العراق.

٤) قدو، سجى جاسم محمد ، (٢٠٠٤)، "كبس إشارة الكلام بواسطة استخلاص الخواص " بحث ماجستير، كلية علوم الحاسبات والرياضيات، جامعة الموصل ، العراق.

5) Barnes C., Bautts T., Lioyd D., Et Al, (2002), "Hack Proofing Your Wireless Network", Published by Syngress, inc.

6) Brooks, David W.; Carr, Adam and Edkins, Keith; et al, (2004), "Data Compression", Wikipedia the Free Encyclopedia, GNU Free Documen -tation License, Boston, U.S.A.

7) **http:// en.wikipedia.org/wiki/.**

8) Dobrian, Christopher, (1997), "Digital Audio", from MSP: The Documentation Cycling' 47 and IRCAM, Dec. 1997.

9) Jan C. A., (1998), "Basic Methods Of Cryptography", published by Cambridge university press.

10) Johnson N. F., Duric Z. and Jajodia S., (2001), "Information Hiding: Steganography And Watermarking – Attack And Countermeasures", published by kluwer academic.

11) Kabal, P., (2004), "Audio File Format Specification", TSP Lab, ECE, McGill University.

12) **http://www.tsp.ecemcgil.ca/mmsp/documents/AudioFormats/**

13) Lee, Jong-hwan; Park, Hyung Min; Jung, Ho-Young, (2002), "Feature Extraction Using Independent Component Analysis", Brain Science Research Center (BSRC), Korea.

14) **http://bsrc.kaist.ac.kr./braintech/image/reports/1year/eng0101a01/eng0101a01-14.htm**

15) McEnary, John, (2001), "Computer in Music/What is Sound?", Lectures/ The Classroom Instructional Materials/Orange Coast College in Costa Mesa, California.

16) **http:// www.occ.cccd.edu/faculty/jmcenary/sound/sound.htm**

17) Schneier B., (1996), "Applied Cryptography", Pblished by Katherine Schowalter, Printed in USA.

18) Seberry J., Pieprzyk J., (1989), "Cryptography An Introduction To Computer Security", Pblished by Pentice hall of Atralia pty ltd.

19) Skilar, Bernard, (2001), "Digital Communication Fndamentals and Application", 2nd edition, Los Angles, Prentice Hall P T R.

20) Stallings W., (1999), "Cryptography And Network Security Principles And Practice", second edition, published by prentice-hall, inc, the USA.