إخفاء المعلومات المرسلة ضمن الإشارات الصوتية العالية الجودة

ساهرة عبيد سعد
كلية العلوم – جامعة البصرة
نجاة حميد قاسم
كلية التربية – جامعة البصرة

الخلاصة:

يتضمن البحث خوارزمية مقترحة لتشفير واخفاء معلومات ضمن الإشارات الصوتية الرقمية العالية الجودة,حيث قامت الخوارزمية بضغط وتشفير الإشارات الصوتية كمرحلة أولى اعتمادا على خوارزمية تحويل الشفرة Modified Discrete Cosine Transform(MDCT) لتحري العناصر التي لاترسل عبر شبكات الاتصال عن بعد broadband network ,قدمت الخوارزمية مفاهيم بالغة الأهمية في تقليص الاشارات الصوتية وتشفيرها في نظام MPEG تضمنت حساب عتبة الحجب للإشارات الصوتية العالية الجودة المسجلة عند تردد 32 KHZ لـــ 16 bit/sample لتوليد الكتل block كل منها بحجم 1024 عينة sample(أي 32 msc), وكمرحلة ثانية تم اخذ معلومات ثم خزنها في ملف نصي,كما ان برنامج التشفير سينفذ على هذا الملف وتولد محتويات جديدة او ملف النص المشفر ,ان عدة برامج فرعية معتمدة على طرائق التشفير التعويضية استخدمت هنا لتحويل النص الى قيم ثنائية(0,1) ومن ثم إخفاءها داخل الملف الصوتي المشفر كمرحلة نهائية ,وعندما يتم استلام الاشارات الصوتية يتم فتح الاشارات وإرجاعها الى اصلها بأمان.

1-المقدمة :

في الوقت الحاضر أصبحت تقنيات تضمين وتشفير الإشارات المرسلة عبر شبكات الاتصال بالغة الأهمية , وذلك للحفاظ على أمنية المعلومات المرسلة,لذا ظهرت عدة تقنيات تضمين وتشفير منها تضمين نص مع صورة او صوت او نص مع صوت...الخ, وكانت هناك عدة خوارزميات مختلفة لاجراء عملية التضمين كل منها لها خصوصيتها.

ولغرض حماية المعلومات العابرة خلال خطوط الاتصال او الأوساط الخزنية فأن المعلومات يمكن ان تخفى او ترمز ,واذا كان نظام الاتصال او نظام الحاسب مبنيا بصورة مثلى ,فأن اي دخول غير شرعي لاستخلاص المعلومات المفيدة من قبل الفرد امرا صعب ويستغرق زمنا طويلا وان اخفاء المعلومات المفيدة في صورة غير مفهومه هو الحلم الذي حققه التشفير[9].

ان الاحتياج لتحسين امن البيانات والمعلومات في انظمة الحاسبات الالكترونية هو نتيجة مباشرة للاستخدام المتزايد للحاسبات من قبل المصانع الحكومية والخاصة في معالجة وخزن وايصال البيانات القيمة والحساسة واضافة الى ذلك فأننا نرى اهتماما حكوميا وعاما في مجال امن البيانات والمعلومات [13],كما ان المخاوف الاخيرة من جرائم الحاسبات والحاجة الى خصوصية المعلومات أدت ايضا الى زيادة الاهتمام في التشفير ليكون وسيلة لاخفاء وحماية البيانات السرية ويمكن للتشفير ان يعطي درجة عالية من الامن بأقل كلفة , وبما ان طرق التشفير التقليدية قد لاتعطينا الدرجة المطلوبة من الامن , لذا فقد تم تطوير تقنيات جديدة بحيث تعطي مستويات عالية من الامن عند تطبيقها على نظام الحاسب وهذه التقنيات الجديدة تستخدم مبادئ طرق التشفير التقليدية ومبادئ رياضية تطبق على الحاسب [11].

2-خوارزمية العمل

العمل الحالي يمر بمرحلتين رئيستين وهي:-

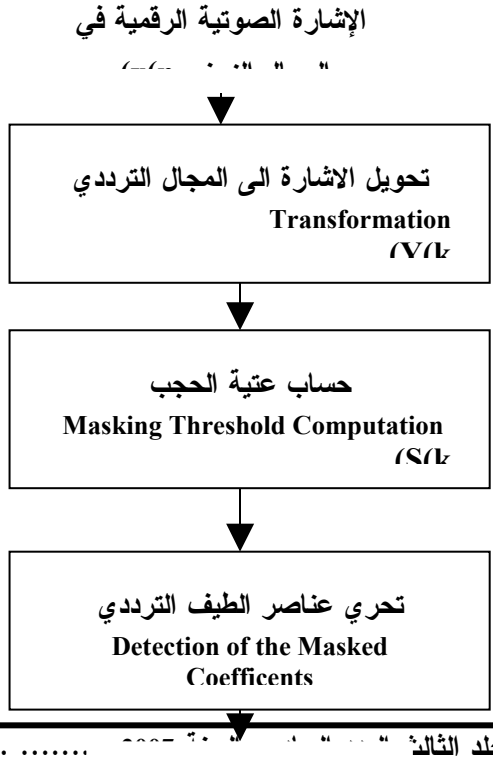
2 .1-مرحلة تحويل الاشارات الصوتية الى القيم الثنائية(تشفيرها)

2.2- مرحلة تشفير النص المدخل وتضمينه ضمن الملف الصوتي.

وفيما يلي شرح لهاتين المرحلتين:-

1.2-مرحلة تحويل الاشارات الصوتية الى القيم الثنائية

الشكل(1) يبين خطوات تحويل الاشارات الصوتية الرقمية الى المجال الترددي digital audio blocks based on MDCT وتشفيرها.



الشكل(1) مراحل تحويل الاشارة الصوتية الرقمية الى المجال الترددي وتشفيرها

وفيما يلي شرح مفصل لهذه الخطوات :-

1.1.2 -تحويل الإشارة الى المجال الترددي :-

تم في هذا البحث تسجيل الاشارات الصوتية باستخدام الحاسب عند تردد 32 KHZ أي (32 msec) للحصول على الاشارات الصوتية في المجال الزمني , بهذه العملية يتم تقطيع الاشارات الصوتية (samples) الى كتل blocks كل منها بحجم 1024 samples عينة أي N=1024 [1,2, samples] وكما يبينها الشكل(2)

بعدها تم تحويل هذه الاشارات الى المجال الترددي بأستخدام خوارزمية (MDCT) وهي حالة خاصة من فورير,هذه الخوارزمية اختزلت الاشارة الى النصف لتصبح (N/2 sample) عينة لتداخل الكتل المتوالية مع بضعها من الطيف الترددي (overlap) كما في الشكل(3)

عملية التحويل معطاة بالمعادلة الاتية: -

$$Y(m,k) = \sum_{n=0}^{N-1} x(n) \cdot h(n) \cos\{2\pi/4n(2k+1)((2n+1)+(2k+1)\pi/4\} \quad \ldots(1$$

where :

N = block size of 1024 samples
m = block number
(k = frequency index (0……N/2-1
x(n) = amplitude of the input sample
−:h(n) = analysis windows defined by

$$h(n) = \sqrt{2} \sin [\pi(n+1/2) / N] , n = 0….N – 1$$

n : sample index

كما ان عملية إرجاع الاشارة الى المجال الزمني inverse transform تتطلب للحصول على x(n) مره اخرى[1,4] كما يلي:− N – 1

$$Xr(m,n) = \sum Y(m,k) . \cos \{2\pi/4N(2k+1)(2n+1)+(2k+1)\pi/4 \} \quad (2)$$

n = 0
n = 0,……..,N – 1

ان الهدف من تحويل الاشارة الى المجال الترددي هو لتحليلها عبر فلتر لمعرفة الاشارات المسموعة وغير المسموعة من الطيف الترددي وهذه العملية غير ممكنه في المجال الزمني.

2.1.2 −حساب عتبة الحجب Masking Threshold Computation

اعتمد حساب عتبة الحجب على الخصائص السمعية او نظام السمع لدى الإنسان (human ear) ونعتبر مهمة في تقنيات ضغط الصوت , بعض الإشارات الصوتية تكون مسموعة والبعض الاخر لا يصل الى الاذن البشرية(غير مسموعة) نتيجة لتغطيتها من قبل الاشارات المجاورة الاعلى منها وهذه الظاهرة تعرف بحجب الاشارات الصوتية في نظم Movie Picture Expert Group (MPEG), حيث تهمل الاشارات غير المسموعة وترسل فقط الاشارات المسموعة وبهذا يتم تقليص الاشارة الصوتية المرسلة[5,8] ,لذا نحتاج الى فلتر لتحوي الاشارة الصوتية

المسموعة وغير المسموعة وذلك يتم بحساب عتبة الحجب وكالاتي:- – M

$$1\ S(m,k) = \sum B(vk - vi)\ Y2(m, i) \quad i = 0$$

حيث Y تحسب من المعادلة (1)

vk ,vi مواقع ترددية للعناصر الترددية k , i في الحزمةالترددية Bark

حيث (Bark = 100 HZ 1)

M = N/2 =512

الشكل(4) بوضح الدالة B(v) وهي دالة تحاكي غشاء الطبلة للاذن البشرية وتعرف كالاتي:-

$$B(v) = \begin{cases} -1/2 <= v <= ½ \text{ Bark} & \Theta dB \\ v > ½ \text{ Bark} & \Theta dB - 10(v - ½) \end{cases}$$

النص الصريح **Text Paint**

عملية ابدال او تحويل الحروف

Bark

3.1.2- تحري عناصر الطيف الترددي

باستخدام عتبة الحجب يتم تحري الاشارة للطيف الترددي وذلك بمقارنة عناصر الطيف الترددي Y(k) مع العتبة S(m,k) حسب المعادلة الاتية:-

$$(Y2(k) < S(m,k$$

فاذا كانت الاشارة اكبر من قيمة العتبة تكون مسموعة واذا كانت اقل تكون محجوبة عن السمع ,وبهذا يتم تشفير الاشارة بـــ 1 اذا كانت مسموعة وصفر اذا كانت محجوبة عن السمع(غير مسموعة)، وبهذا تم تحويل الاشارة الى شفرات من الصفر والواحد ليتم معالجتها في المرحلة اللاحقة وتضمينها الاشارات النصية[1].

2.22-عمليات تشفير النص المدخل وتضمينه في الملف الصوتي

الشكل(5)يبين خطوات تشفير النص الصريح:-

وفيما يلي شرح مفصل لخطوات التشفير:-

2.21.-عملية ابدال او تحويل الحروف

ان عملية التبديل تتم بأخذ كل ستة حروف متتالية من النص ووضعها في صناديق التبديل (s1,.....s6) وإجراء عملية التبديل عليها وكما موضح في المثال الاتي:-

الناتج	الكلمة	موقع التبديل	الموقع الابتدائي
y	2	4	
S			
	y	4	2
			S
S		5	3
E			
T		6	4
M	5	1	E
S			
M	2	6	أي ان

الحرف الرابع يتم وضعه بالموقع الاول والحرف الثالث بالموقع الثاني وهكذا مع الحرف الثاني في الموقع السادس او الاخير.

2.2.2 –عملية تحويل وتغير الحروف

في هذه العملية يتم اختيار كلمة السر(أي الكلمة المفتاحية),فمثلا تم ادخال كلمة السر مثل STAR WARS ,ومن ثم تكتب كلمة السر على شكل حروف متصلة لا توجد بينها فراغات

وتهمل الحروف المتكررة فيها ويتم توزيع حروف الكلمة على القطر الرئيسي للمصفوفة(ويستخدم القطر الثانوي في حالة الحاجة لتكملة حروف كلمة السر), ومن ثم تكتب الحروف الانكليزية الـــ (26) حرف **الغير** موجودة في كلمة السرلتكملة المصفوفة سطر_سطر ,وكما موضح:-

S B C D E
F T G H I
J K A L M
N O P R Q
U V X Y W
Z

ثم تقرا من المصفوفة بصورة متدرجة من اليسار الى اليمين وبضمنها كلمة السر,وتكتب الحروف المقروءة بشكل سطر تحت الحروف الانكليزية ,حيث تقرا الحروف في الخط المائل من الاعلى الى الاسفل (يجب ان تكون عناصر المصفوفة 26 حرفا) وكما يلي:-

ABCDEFGHIJKLMNOPQRSTUVWXYZ
EDICHMBGLQSTARWFKPYJOXNVUZ

ولعمل التشفير تقرا الحروف من الاعلى الى الاسفل (أي تقرا الحروف في تسلسل الابجدية الانكليزية)وما يناظره اسفله يكون هو الحرف المطلوب والذي نكتبه ,فمثلا اذا كان النص الصريح

I HAVE TWO BOOKS
L GEXH JNW DWWSY

ومن ثم يتم تقسيم الحروف الناتجة الى مجاميع وبطول كلمة السر المدخلة وكما يلي:-

L	G	E	X	H	J	N	W
S	T	A	R	W	A	R	S
D	Z	E	O	D	J	E	O

D	W	W	S	Y			
S	T	A	R	W	A	R	S
V	P	W	J	U			

وبأخذ الابجدية وترقيمها وكما يلي:-

20 19 18 17 16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1 0
26 25 24 23 22 21
A B C D E F G H I J K L M N O P Q R S T U V
W X Y Z

ومن ثم تطبق العلاقة الاتية:-

$F(a) = (a + k) \bmod 26$ .....(3

حيث ان a تمثل الموقع القديم للحرف وان k تمثل موقع المفتاح , فأن الناتج من العلاقة (3) يمثل موقع الحرف المشفر ومع مراعاة الـــ mode في حالة تجاوز الجمع الرقم 26, فكان ناتج التشفير :-
DZEODJEOVPWJU

3.2.2 -عملية تحويل الحروف الى الثنائيات المقابلة

ان الحروف الناتجة من العملية السابقة يتم تبديل كل حرف باقيمه اسكي المناظرة له ,ومن ثم يأخذ كل قيمه من القيم الناتجة (أي كل بايت) ويجري عليها تفكيك الى الثنائيات المكونه لها ,حيث اعتمدت عملية التفكيك على تطبيق العامل and علىكل بايت ومع المعيار $80 أي ان byte and $80

وملاحظة الناتج اما صفر او واحد وإجراء عملية الازاحة بمقدار واحد الى اليسار(shift) واعادة تطبيق العامل and ومع القيمة ($80) على البايت المزحف وهكذا الى نهاية البايت ,فمثلا اذا كان البايت يحوي على الرقم 5

0	0	0	0	0	1	0	1

1	0	0	0	0	0	0	0

وبتطبيق العامل and نحصل على القيمة صفر وبعد هذا نقوم بعمل تزحيف البايت الى اليسار وتستمر هذه العملية الى ان نحصل على الشفرة الكاملة للبايت الحالي هي(000000101) ومن خلال هذه العملية يتم تحويل قيم اسكي المخزونه في البايت الى الثنائيات المقابلة لها.

4.2.2-عمليات التعويض والعكس للقيم الثنائية

يتم في هذه الخطوه اجراء مجموعة من العمليات على القيم الثنائية الناتجة من المرحلة السابقة , ومن هذه العمليات عملية التعويض ويتم في هذه العملية اخذ كل ثمانية ثنائيات متتالية ووضعها في صناديق التعويض (s1, s8,.....) (من اليسار الى اليمين) واجراء عملية تعويض للقيم , حيث يتم عكس قيم هذه الثنائيات ,فمثلا الثنائيات (01010111) يتم تحويلها(10101000) ,وبعد اكمال هذه العملية على كل الثنائيات يتم ادخال هذه

الثنائيات الناتجة بعملية اخرى وهي عملية العكس للقيم الثنائية , وتتم بأخذ كل ثماني ثنائيات متتالية)ومن اليسار الى اليمين) ووضعها في صناديق العكس(s1,.....,s8) ويجري عليها عكس لترتيبها , فمثلا اذا كانت الثنائيات الناتجة من العملية السابقة(10101000) تحول الى(00010101) , ان الغرض من هذه الخطوه وما تضمنته من عمليات على الثنائيات هي زيادة التعقيد على مهاجم النص للوصول الى الثنائيات الحقيقية للنص .

3-اخفاء بيانات النص ضمن الملف الصوتي :

ان ناتج المرحلتين الرئيستين للنظام ,أي مرحلة تحويل الاشارات الصوتية الى القيم الثنائية ومرحلة تشفير النص المدخل هي قيم ثنائية (0,1) وفي النهاية يتم اخفاء معلومات النص والتي تتم تحويلها الى سلسلة من الثنائيات داخل ملف الصوت ,حيث يتم وضع كل بيانات الملف النصي بدلا من القيم الصفرية والتي تمثل الاماكن الغير مسموعة في الملف ,ان هذه الطريقة تفيد من الناحية الامنية ,حيث تحافظ على النص مخبأ ضمن الاشارات الصوتية دون التأثير على جودتها وعند التسليم يتم فتح الاشارات وارجاعها الى اصلها بأمان.

4-النتائج والمناقشة والاستنتاجات:

من خلال التطبيق العملي تم استنتاج الحقائق الاتية:-

بعد ان تم تسجيل الاشارات الصوتية بواسطة الحاسب عند تردد 32 KHZ حصلنا على اشارة بالمجال الزمني وبحجم 16 بت لكل عينة sample هذه العينات ولدت كتل blocks بحجم 1024 عينه وهذه الاشارة ممثلة في الشكل (2)، ولكي تحول هذه الاشارات الى المجال الترددي استخدمنا خوارزمية MDCT للحصول على عناصر الطيف الترددي Y(k) كما في الشكل(3) , استخدمت هذه الخوارزمية لتقليص الاشارة الى النصف

ليصبح عدد عناصر كل كتلة تساوي (N/2 = 512) عينة وهذه العملية تجعل التحري عن الاشارة المحجوبة عن السمع اكثر سهولة ومرونة ,كما ان التمثيل الترددي للاشارة يستخدم لفحص الخصائص السمعية التي تم الاعتماد عليها لتحري الاشارة الغير المسموعة (التي لاترسل) المتأثرة بعملية الحجب Masking كما ان عتبة الحجب Masking Threshold تم حسابها اعتمادا على تجربة عدة قيم للرمز Θ الذي يمثل عتبة الحجب عند الهدوء quietness threshold او نسبة الاشارة الى الحجب signat to mark ratio والتي تعني نسبة بين الاشارة وعتبة الحجب , بحيث اثبتت التجربة ان عتبة الحجب تزداد كلما زادت قيمة Θ , على سبيل فاذا كانت 0 >= Θ , فان كل عناصر الطيف الترددي تحجب وذلك لان طاقة الحجب تزيد عن 100 db وهذا غير منطقي لذا فان التجربة اثبتتت ان القيمة = −30 Θ هي مناسبة جدا لحساب عتبة الحجب الشكل(6) يوضح التجربة على عدة قيم لـــ Θ

, بعد ان تم تحري عناصر الطيف الترددي يتم التعرف على مواقع العناصر الترددية المحجوبة عن السمع

وكذلك عددها لكي يتم تصفيرها ومن ثم استخدامها للمرحلة اللاحقة للعمل وهي اخفاء شفرة نص ضمن هذه المواقع ثم ارسالها حيث ان فهرست هذه المواقع مهم جدا لعملية اعادة الاشارة عند الاستلام.

ولغرض توضيح عملية تشفير النص تم اخذ الملف النصي والذي يحوي على المعلومات الاتية:−

رقم	الاسم	العنوان

101	Jones Tool Co	Chicago,IL	60605.
102	HAL Computers ,Inc	Armonk,NY	10504.
103	Going Systems Group	Seattle,WA	98124.
104	TOH Steel Co	Pittsburgh,PA	15213.
105	Cipher System,Inc	Arlington,VA	22209.
106	G & O Co,Inc	Houston,TX	77002.
107	LSI Co, Inc	New Haven,CT	06520.
108	I/O Devices Corp,	Holmdel,NJ	07733.
109	CRT Inc,	Fresno,CA	93710
110	Crypto Systems,Ltd	Rockville,MD	20852.

حيث ادخل الملف السابق الى عملية التبديل للحروف وذلك بأخذ كل ستة حروف متتالية ومن اليسار الى اليمين وإجراء عملية التحويل او التبديل وحسب مفتاح المزج المحدد(435612) مع ملاحظة ان الحروف الاخيرة اذا كانت اقل من ستة تترك كما هي بدون تحويل اوتبديل فكانت النتائج التي حصلنا عليها كما يلي:-

```
 1  10oJne  T oos oC  l      ciagChLI  o,6 06  012 05   H  C omALetrspunIc
mo  N,Y nk   1  401005    3 nig GotsemSyrGous   Sep lte,at    WA8912  40  41T
  etel S o   C      tits Pgrh,bu   1PA311052    5 hperCisyte SnIc m,  Ar  gnt
AV  n,2 22  016 09  G    OCo& cn  ,I      oHus  ,nTXto      0702 7 7  10SLI
InCo    c       wHaNe,nCTve   0  021065    8  ODeI/ecs vipr, Co  Ho  edl,lm
NJ0 77  019 33  CR  nIc,T           rFes  C,A no      7310 9110
  Cr  ot Sypetmsys,Ltd_
```

ومن ثم ادخلت الحروف الناتجة من العملية السابقة الى عمليات التحويلات وتغيرات للحروف واعتمادا على كلمة السر المدخلة والتي كانت STAR WARS فكانت النتائج التالية:-

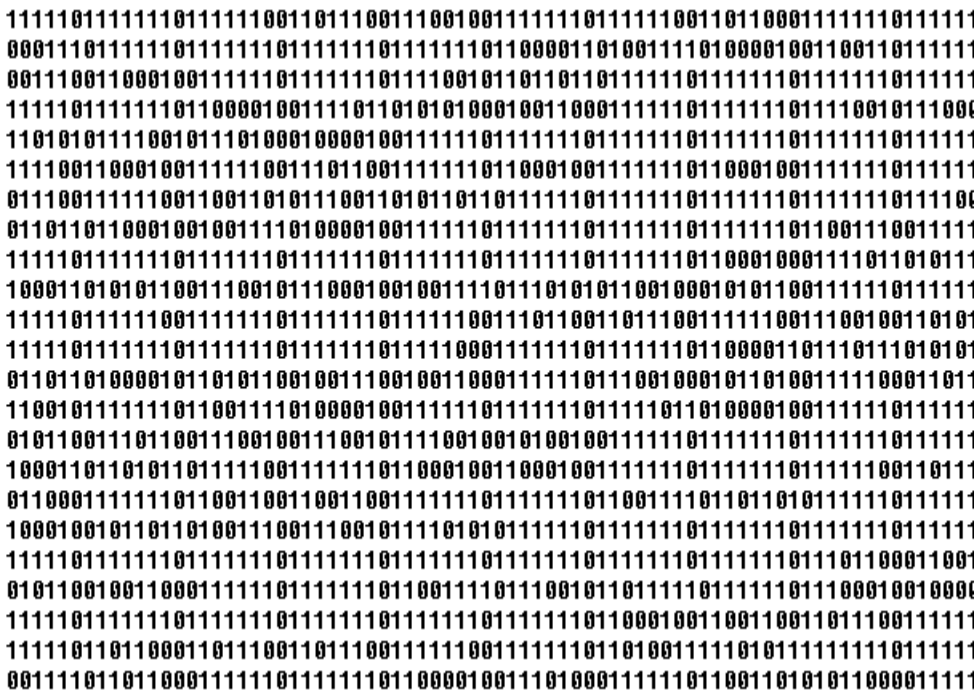
وبتقسيم الحروف الناتجة الى مجاميع وبطول كلمة السر واستخراج الحروف حسب العلاقة(3)السابقةنحصل على النتائج الاتية:-

```
3249323249481117411010132328432111111115321116732321083232323232329910597
1047673323211144543248543232484950324853323232723232673211110965761011161141
2117110739932324411465109111323278448932110107323232493232524849484853323232
3211010510332711111161151011098312111471111117115323232831011123210811610144
6323232328765565749503232524832325249843279723232101116101108328332111323232
3232323232116105116115328010311410444981173232324980655149494853503232323253
4112101114671051151211161013283110739932109443232651143232103110116111108105
3232110445032505032324849543248573232713232323279671113832991103232447332323
2321117211711532324411084881161113232323232324855485032553255323249488376733
2324473110671113232323299323232323232323211972977810144110678411810132323248
4850494854533232323256323279681017347101991153211810511211444326711132327217
```

```
 1  10oQkm  S wys wY  e      moikMoQS  q,6 06  012 05   I  O suOQsuwyacwYa  ,iK
eg  M,Q mo   1  401005    3 kmo KmoqsuWysUwya   Ace ikm,ik    UW8912  40  41G KM
  kmoq U q   Y      egik Gikm,qs   1UW311052    5 gikmOqkmoq UwYs w,  Eg  egikmo
IK  q,2 22  016 09  G    IKm& su  ,U      aCeg  ,gIKmo      0702 7 7  10CEG    ,
KmOq    s       cEgIk,oIKmo   0  021065    8  MGiK/oqs oqsu, Ac  Ac  ike,ik
MO0 77  019 33  CE  kMo,K           eGac  I,M ik      7310 9110
  Km  km Qsuoqsuwy,Cwy
```

ومن ثم تم تحويل القيم السابقة الى الثنائيات المقابلة لها كما يلي:-

ومن ثم تم إجراء عدة عمليات على هذه الثنائيات فالعملية الاولى عملية التعويض حيث تم تعويض (0)بالـــ(1) فكانت النتائج كما يلي:-



وبعد ذلك تم إجراء عملية عكس حيث تم أيضا تم اخذ كل ثمانية ثنائيات متتالية ومن اليسار الى اليمين فكانت النتائج كما يلي:-

المصادر:

[1] Y.Mahienx and J.P.Petit ,"High-Quality Audio Transform coding at 64 kbps " ,IEEE Trans on comm.,vol.42,No.11,pp.3010-3019,Nov.,1994.

[2] T.Kintzle, "Guide to Sound " , Addison-wesly , England , 1998.

[3] P.A.Lynn,Introductory Digital signal processing with computer Applications,1997.

[4] K.Hosoda , O.Noguchi and Y.Yatsuzuka , "A 32 Kbit/s ADPCM Algorithm Having High Performance for both Voice and 9.6 Kbit/s modern signals ",IEEE JOUR. On selected Area in communi.,Vol.6,No.2,Feb., 1988.

[5] M.Orzessek and P.sommer,ATM & MPEG-2 Integrating Digital Vidio into Broadband networkes 1998.

[6] M.R.Portnoff,"Time-Frequency Representation of Digital signals and systems based on short-time fourier analysis ",IEE Trans. On Aconstic ,speech and signal processing vol.Assp-28,no.1,1980.

[7]-W.Buchman , "Advanced Data Communications and Networks" , chapwan and hall , Landon , 1997.

[8] J-Watkinsan, "Compression in Video and Audio " , Great Britain , British library ,1997.

[9] Beker H. & piper F. ,"Cipher Systems The Protection of Communications",Nothwood publications,U.K.,1982.

[10] Seberry J. & Pieprzyk J. ,"Cryptography An Introduction to computer Security",prentice-Hall Inc.,U.S.A,1989.

[11] Dennig D.E.R , "Cryptography and data security ,Addison-wesley publishing company Inc.,U.S.A., 1982.

[12] بروس بوزورت ،"الرموزالشفرات والحاسبات مقدمة الى آمن المعلومات" , الطبعة الاولى،1989.

[13] الحمداني ،وسيم عبد الامير، "ا نظمة التشفير" ،الطبعة الاولى،1992.

[14] د.وسيم عبد الاميو الحمداني وسن شلكر عواد ، "انظمة التشفير الانسيابي ",كتاب غير منشور,بغداد,1997.

[15] Schneier B. , "Applied Cryptography protecols, Algorithm and source code in c ", John wiley and sons ,Inc.,U.S.A,1996.

Hiding transmitted information within high quality digital audio

Sahira.A.Sead
Basrah University - college of Science
Najat.H.Qassim
Basrah University - college of Education

: Abstract

In this paper we introduce Algorithm to encode and hid un information within high quality digital audio signals . first, The digital audio signals are compression and encoded based on MDCT (Modified Discrete Cosine Transform) Algorithm , to investigate the masked coefficients of the spectrum that are assumed to be not transmitted in the basic access of broadband network ,the proposed algorithm introduced the most significant concepts in high-quality digital audio encoding or compression in MPEG systems. It involves computers masking curve s(v) of high quality digital audio signals which are experimentally recorded at 32 KHZ sampling rate and quantization of 16 bit/sample to generate blocks , each with size of 1024 samples (32 msec duration).

Second the information of text are scanned in file to encoding it into encode text file ,this file are encoded into(0,1)bit using many sub-programes to intered it with audio file codes in the recever the decoding program.