إخفاء المعلومات المرسلة ضمن الإشارات الصوتية العالية الجودة

ساهرة عبيد سعد
كليه العلوم – جامعه البصرة
نجاة حميد قاسم
كليه التربيه – جامعه البصرة

الخلاصه:

يتضمن البحث خوارزميه مقترحه لتشفير واخفاء معلومات ضمن الإشارات الصوتيه الرقميه العاليه الجودة،حيث قامت الخوارزميه بضغط وتشفير الإشارات الصوتيه كمرحله اولى اعتمادا على خوارزميه تحويل الشفرة Modified Discrete Cosine Transform(MDCT) لتحري العناصر التي لاترسل عبر شبكات الاتصال عن بعد broadband network ،قدمت الخوارزميه مفاهيم بالغه الاهميه في تقليص الاشارات الصوتيه وتشفيرها في نظام MPEG تضمنت حساب عتبه الحجب للإشارات الصوتيه العاليه الجودة المسجله عند تردد 32 KHZ لـ 16 bit/sample لتوليد الكتل block كل منها بحجم 1024 عينة sample(اي 32 msc)، وكمرحله ثانيه تم اخذ معلومات تم خزنها في ملف نصي،كما ان برنامج التشفير سينفذ على هذا الملف وتولد محتويات جديدة او ملف النص المشفر ،ان عدة برامج فرعيه معتمدة على طرائق التشفير التعويضيه استخدمت هنا لتحويل النص الى قيم ثنائيه(0,1) ومن تم إخفاءها داخل الملف الصوتي المشفر كمرحله نهائيه ،وعندما يتم استلام

الاشارات الصوتيه يتم فتح الاشـــارات وإرجاعها الى اصلها بامان.

١ - المقدمة :

في الوقت الحاضر اصبحت تقنيات تضـــمين وتشـــفير الإشـــارات المرسلة عبر شبكات الاتصال بالغة الاهمية ، ودلك للحفـــاظ علـــى امنيـــة المعلومات المرسلة،لذا ظهرت عدة تقنيات تضمين وتشفير منها تضمين نص مع صورة او صوت او نص مـــع صـــوت...الـــخ، وكانـــت هنـــاك عـــدة خوارزميات مختلفة لاجراء عملية التضمين كل منهـــا لهـــا خصوصـــيتها. ولغرض حماية المعلومات العابرة خـــلال خطـــوط الاتصـــال او الاوســـاط الخزنية فان المعلومات يمكن ان تخفى او ترمز ،واذا كان نظام الاتصال او نظام الحاسب مبنيا بصورة مثلى ،فان اي دخول غير شرعي لاســـتخلاص 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 والمعلومـــات فـــي انظمـــة الحاســـبات الالكترونية هو نتيجة مباشرة للاستخدام المتزايد للحاسبات من قبل المصانع الحكومية والخاصة في معالجة وخزن وايصال البيانات القيمـــة والحساســـة واضافة الى دلك فاننا نرى اهتماما حكوميا وعاما في مجال امـــن البيانـــات والمعلومات [13]،كما ان المخاوف الاخيرة من جرائم الحاسبات والحاجـــة الى خصوصية المعلومات ادت ايضا الى زيادة الاهتمام في التشفير ليكـــون وسيلة لاخفاء وحماية البيانات السرية ويمكن للتشفير ان يعطي درجة عاليـــة من الامن باقل كلفة ، وبما ان طرق التشفير التقليدية قد لاتعطينـــا الدرجـــة المطلوبة من الامن ، لدا فقد تم تطوير تقنيات جديدة بحيث تعطي مســـتويات عالية من الامن عند تطبيقها على نظام الحاسب وهـــده التقنيـــات الجديـــدة

تستخدم مبادئ طرق التشفير التقليدية ومبادئ رياضية تطبق على الحاسب]١١[.

٢-خوارزميه العمل

العمل الحالي يمر بمرحلتين رئيستين وهي:-

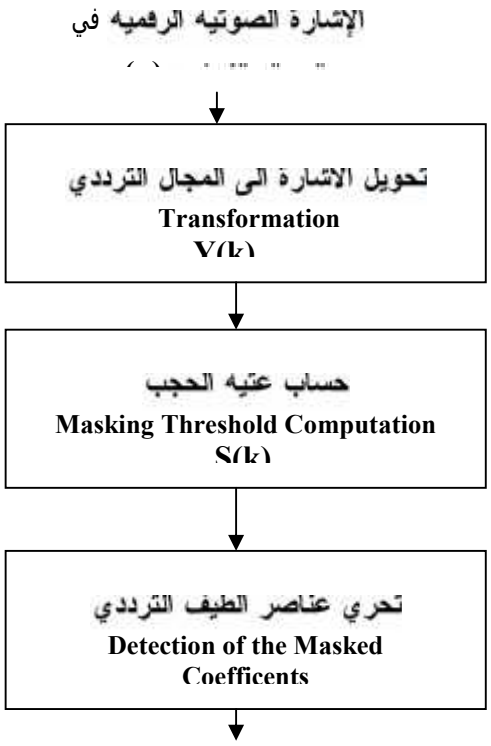
٢ .١-مرحلة تحويل الاشارات الصوتية الى القيم التنائية(تشفيرها)

٢.٢- مرحلة تشفير النص المدخل وتضمينه ضمن الملف الصوتي.

وفيما يلي شرح لهاتين المرحلتين:-

١.٢-مرحلة تحويل الاشارات الصوتية الى القيم التنائية

الشكل(١) يبين خطوات تحويل الاشارات الصوتية الرقمية الى المجال الترددي digital audio blocks based on MDCT وتشفيرها.



وفيما يلي شرح مفصل لهذه

الشكل(١) مراحل تحويل الاشاره الصوتيه الرقميه الى المجال الترددى وتشفيرها

١.١.٢ -تحويل الإشارة الى المجال الترددي :-

تم في هذا البحث تسجيل الاشارات الصوتية باستخدام الحاسب عند تردد 32 KHZ اي (32 msec) للحصول على الاشارات الصوتية في المجال الزمني ، بهذه العملية يتم تقطيع الاشارات الصوتية (samples) الى

كتل blocks كل منهـا بحجـم 1024 samples عينـة اي N=1024 samples ، [1,2] وكما يبينها الشكل(٢)

بعدها تم تحويل هذه الاشـارات الـى المجـال التـرددي باسـتخدام خوارزمية (MDCT) وهي حالة خاصة من فـوريرهـذه الخوارزميـة اختزلت الاشارة الى النصف لتصبح (N/2 sample) عينة لتـداخل الكتـل المتوالية مع بضعها من الطيف الترددي (overlap) كما في الشكل(٣)

عملية التحويل معطاة بالمعادلة الاتية: -

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

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:-

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

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

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

٢.١.٢ -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 لتحري 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

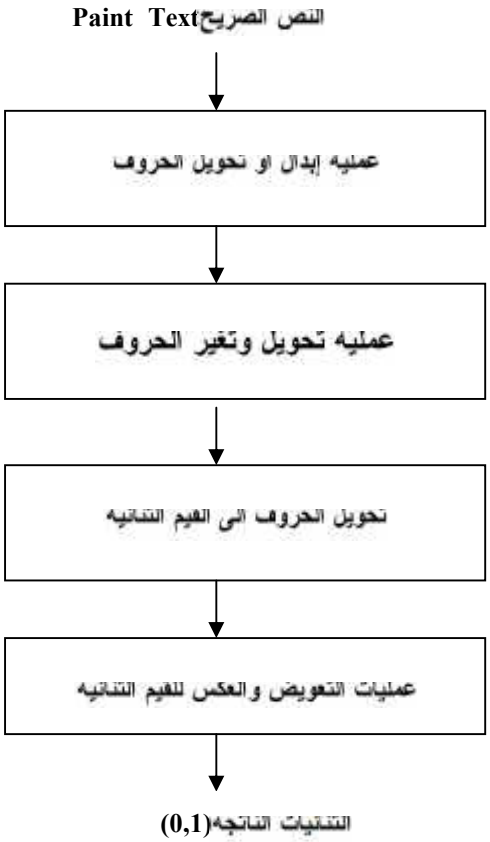
حيث (1 Bark = 100 HZ)

$$\mathbf{M = N/2} = 512$$

الشكل(٤) بوضح الدالة B(v) وهي دالة تحاكي غشاء الطبلة للاذن البشرية وتعرف كالاتي:-

$$B(v) = \begin{cases} \Theta dB & -1/2 <= v <= ½ \text{ Bark} \\ \Theta dB - 10(v - ½) & v > ½ \text{ Bark} \\ \Theta dB + 27(v+1/2) & v < -1/2 \text{ Bark} \end{cases}$$

حيث Θ نسبة الاشارة الىالحجـــب signal –to-mask ratio(SMR) .[1]



وفيما يلي شرح مفصل لخطوات التشفير:-

١.2.2-عملية ابدال او تحويل الحروف

ان عملية التبديل تتم باخذ كل ستة حـــروف متتاليـــة مـــن الـــنص ووضعها في صناديق التبديل (s1,.....s6)وإجراء عملية التبديل عليها وكما موضح في المثال الاتي:-

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

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

٢.٢.٢ -عملية تحويل وتغير الحروف

في هذه العملية يتم اختيار كلمة السر(اي الكلمة المفتاحية)،فمثلا تـــم ادخال كلمة السر مثل STAR WARS ،ومن تم تكتب كلمة الســـر علـــى شـــــكل حـــــروف متصـــــلة لا توجـــــد بينهـــــا فراغـــــات وتهمل الحروف المتكررة فيها ويتم توزيع حروف الكلمـــة علـــى القطـــر الرئيسي للمصفوفة(ويستخدم القطر الثانوي في حالة الحاجة لتكملة حـــروف كلمة السر)، ومن تم 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

تم 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 ٢٦ حرفا) وكما يلي:-

ABCDEFGHIJKLMNOPQRSTUVWXYZ

EDICHMBGLQSTARWFKPYJOXNVUZ

ولعمل التشفير تقرا الحروف من الاعلى الى الاسفل (اي تقرا الحروف في تسلسل الابجدية الانكليزية)وما يناظره اسفله يكون هو الحرف المطلوب والدي 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			

وباخذ الابجدية وترقيمها وكما يلي:-

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26

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 تم تطبق العلاقة الاتية:-

F(a) =(a +k) mod 26 .....(3)

حيث ان a تمثل الموقع القديم للحرف وان k تمثل موقع المفتاح ، فان الناتج من العلاقة (٣) يمثل موقع الحرف المشفر ومع مراعاة الـ mode في حالة تجاوز الجمع الرقم ٢٦، فكان ناتج التشفير :-

DZEODJEOVPWJU

٣.٢.٢ -عملية تحويل الحروف الى التنائيات المقابلة

ان الحروف الناتجة من العملية السابقة يتم تبديل كل حرف باقيمه اسكي المناظرة له ،ومن تم ياخذ كل قيمه من القيم الناتجة (اي كل بايت) ويجري عليها تفكيك الى التنائيات المكونه لها ،حيث اعتمدت عملية التفكيك على تطبيق العامل and علىكل بايت ومع المعيار $80 اي ان

byte and $80

وملاحظة الناتج اما صفر او واحد وإجراء عملية الازاحة بمقدار واحد الى اليسار (shift) واعادة تطبيق العامل andومع 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 التنائيات المقابلة لها.

٤.٢.٢-عمليات التعويض والعكس للقيم التنائية

يتم في هذه الخطوه اجراء مجموعة من العمليات على القيم التنائية الناتجة من المرحلة السابقة ، ومن هذه العمليات عملية التعويض ويتم في هذه العملية اخذ كل ثمانية تنائيات متتالية ووضعها في صناديق التعويض (s1,.....,s8) (من اليسار الى اليمين) واجراء عملية تعويض للقيم ، حيث يتم عكس قيم هذه التنائيات ،فمثلا التنائيات (01010111) يتم تحويلها (10101000) ،وبعد اكمال هذه العملية على كل التنائيات يتم ادخال هذه التنائيات الناتجة بعملية اخرى وهي عملية العكس للقيم التنائية ، وتتم باخذ كل ثماني تنائيات متتالية)ومن اليسار الى اليمين) ووضعها في صناديق العكس(s1,.....,s8) ويجري عليها عكس لترتيبها ، فمثلا اذا كانت التنائيات الناتجة من العملية السابقة (10101000) تحول الى (00010101)، ان الغرض من هذه الخطوه وما تضمنته من عمليات على التنائيات هي زيادة التعقيد على مهاجم النص للوصول الى التنائيات الحقيقية للنص .

3-اخفاء بيانات النص ضمن الملف الصوتي :

ان ناتج المرحلتين الرئيستين للنظام ،اي مرحلة تحويل الاشارات الصوتية الى القيم التنائية ومرحلة تشفير النص المدخل هي قيم تنائية (0,1)

وفي النهاية يتم اخفاء معلومات النص والتي تتم تحويلها الى سلسلة من التنائيات 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 مخبا ضمن الاشارات الصوتية دون التاثير على جودتها وعند التسليم يتم فتح الاشارات وارجاعها الى اصلها بامان.

٤ -النتائج والمناقشه 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 (٢)، ولكي تحول هذه الاشارات الى المجال الترددي استخدمنا خوارزمية MDCT للحصول على عناصر الطيف الترددي Y(k) كما في الشكل(٣) ، 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) المتاثرة 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 فادا كانت ٠ =<

Θ ، فان كل عناصر الطيف الترددي تحجب ودلك لان طاقة الحجب تزيد عن 100 db وهذا غير منطقي لذا فان التجربة اثبتت ان القيمة 30- = Θ هي مناسبة جدا لحساب عتبة الحجب الشكل(٦) يوضح التجربة على عدة قيم لـ Θ

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

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

ولغرض توضيح عملية تشفير النص تم اخد 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.

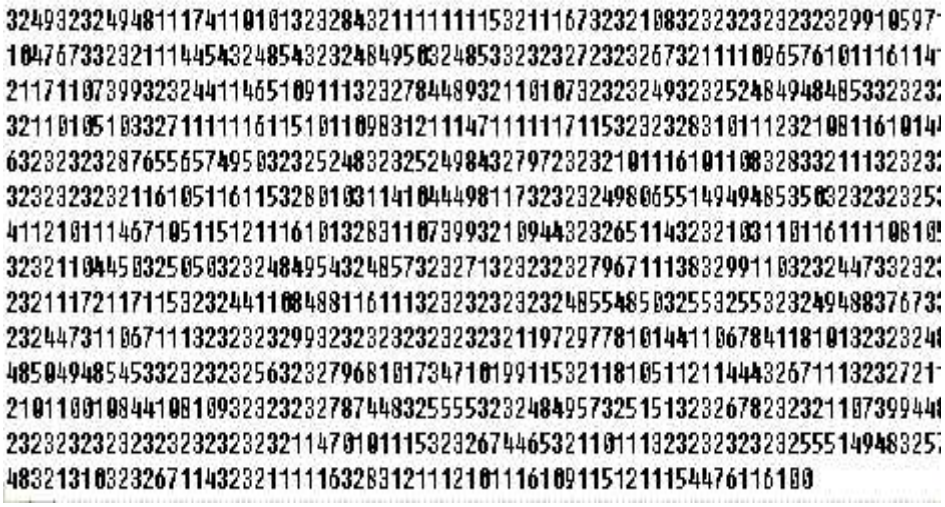
حيث ادخل الملف السابق الى عمليه التبديل للحروف ودلك باخد كل سته حروف متتاليه ومن اليسار الى اليمين وإجراء عمليه التحويل او التبديل وحسب مفتاح المزج المحدد(435612) مع ملاحظه ان الحروف

الاخيرة اذا كانت اقل من سته تترك كما هي بدون تحويل اوتبـــديل فكانـــت النتائج التي حصلنا عليها كما يلي: -

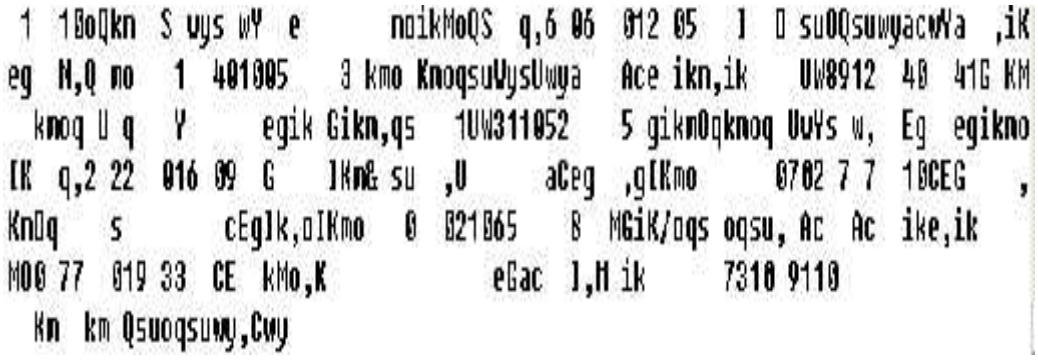
```
 1  10oJne  T oos oC  l       ciagChLI  o,6 06  012 05   H  C onALetrspunlc
mo  N,Y nk   1  401005    3 nig GotsenSyrGous   Sep lte,at    WA8912  40  41T
  etel S o   C      tits Pgrh,bu   1PA311052    5 hperCisyte Snlc m,  Ar  gnt
AV  n,2 22  016 09  G    OCo& cn  ,[      oHus  ,nTXto      0702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

ومن تم ادخلت الحروف الناتجه من العمليه السابقه الى عمليـــات التحـــويلات وتغيرات للحروف واعتمادا على كلمه السر المدخله والتي كانت STAR WARS فكانت النتائج التاليه: -

وبتقسيم الحروف الناتجه الى مجاميع وبطول كلمه السر واستخراج الحروف حسب العلاقه(٣)السابقةنحصل على النتائج الاتيه:-

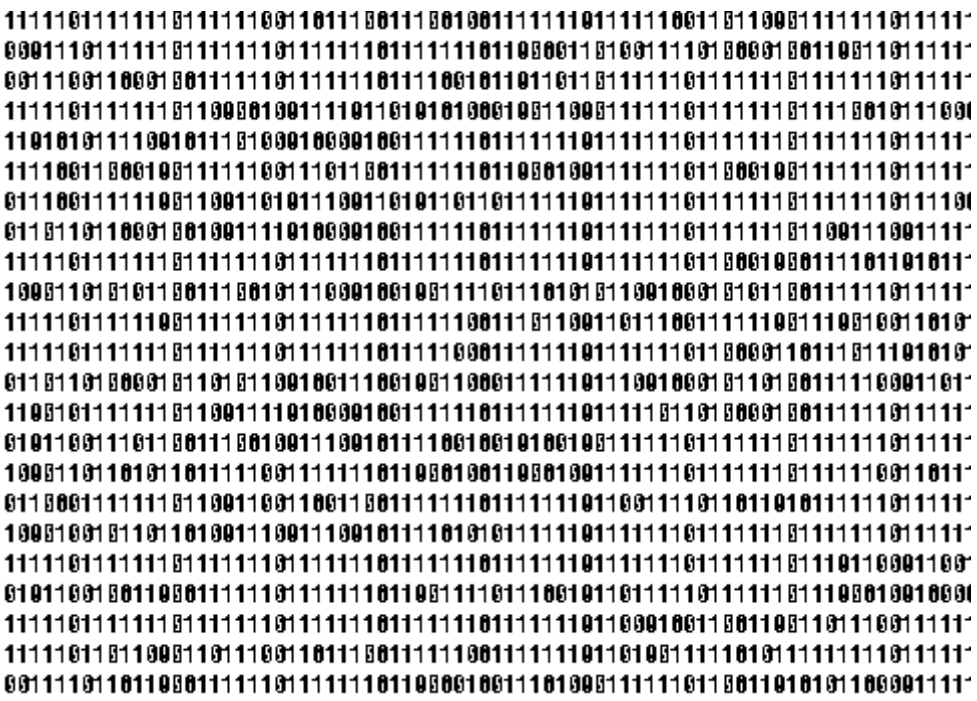


ومن تم ادخلت النتائج السابقه الى عمليه التحويل الى قيم اسكي وكما يلي:-



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

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



وبعد ذلك تم إجراء عمليه عكس حيث تم ايضا تم اخذ كل ثمانيه ثنائيـــات متتاليـــه 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 امن المعلومات" ، الطبعة الاولى،١٩٨٩.

[13] الحمداني ،وسيم عبد الامير، "ا نظمة التشفير" ،الطبعة الاولى،١٩٩٢.

[14] د.وسيم عبد الامير الحمداني وسن شاكر عواد ، "انظمة التشفير الانسيابي "،كتاب غير منشور،بغداد،١٩٩٧.

[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.