

بسم الله الرحمن الرحيم
جامعة السودان للعلوم والتكنولوجيا
كلية علوم الحاسوب وتقانة المعلومات

إخفاء المعلومات السرية في ملف صوتي

Hiding secret information in Audio file

اغسطس/2014

إعداد الطلاب:

- 1- فضل المولى مصطفى .
- 2- مازن كرار حسب الرسول .
- 3- محمد هاشم أحمد محجوب.

مشروع مقدم كأحد متطلبات الحصول على بكالوريوس الشرف في علوم الحاسوب

التاريخ
/ أغسطس /2014

توقيع الأستاذ المشرف
د.طلعت محي الدين وهبي

الآية

(اِقْرَأْ بِاسْمِ رَبِّكَ الَّذِي خَلَقَ * خَلَقَ الْإِنْسَانَ مِنْ عَلَقٍ * اِقْرَأْ وَرَبُّكَ الْأَكْرَمُ * الَّذِي عَلَّمَ بِالْقَلَمِ * عَلَّمَ الْإِنْسَانَ مَا لَمْ يَعْلَمْ)

الحمد لله

الحمد لله الذي شرع لنا الدعاء، وفتح لنا باب الرجاء، نحمده تعالى على كل فضل راح وجاء، ونشكره سبحانه على النعم والآلاء. ونشهد أن لا إله إلا الله وحده لا شريك له، السميع المجيب، يسمع النداء و هو فوق السماء.

نشهد أن سيدنا و نبينا محمدا عبده و رسوله، بين الأدواء و عين الدواء و صلى الله و سلم وبارك عليه، و على آله الأصفياء، وأصحابه الأتقياء، والتابعين و من تبعهم بإحسان، الداعين ربهم في السراء و الضراء.

الاهداء

إلى من جرع الكأس فارغاً ليسقيني قطرة حب
إلى من كَلَّت أنامله ليقدّم لنا لحظة سعادة
إلى من حصد الأشواك عن دربي ليمهد لي طريق العلم
إلى القلب الكبير
إلى أبائنا الأعزاء:

كرار حسب الرسول محمد

مصطفى محمد صالح

هاشم أحمد محجوب

إلى من أرضعتني الحب والحنان
إلى رمز الحب وبلسم الشفاء
إلى القلب الناصع بالبياض
إلى أمهاتنا الفاضلات:

حنان أمين علي

آمنة علي منصور

الزينة محمد إبراهيم

إلى القلوب الطاهرة الرقيقة والنفوس البريئة إلى رياحين حياتي إخوتنا و أخواتنا.
الآن تفتح الأشرعة وترفع المرساة لتتطلق السفينة في عرض بحر واسع مظلم هو بحر الحياة وفي هذه الظلمة لا يضيء إلا قنديل الذكريات ذكريات الأخوة
البعيدة إلى الذين أحببتهم وأحبوني اصدقاءنا الأعزاء.

شكر و عرفان

الشكر أولاً وأخيراً لله سبحانه وتعالى الذي أكرمنا بتوقيفه في إنجاز هذا العمل المتواضع و الشكر أجزله للأساتذة الكرام بجامعة السودان للعلوم و التكنولوجيا- كلية علوم الحاسوب وتقانة المعلومات:

الدكتور طلعت محي الدين الذي أشرف على هذا العمل، وتقديمه العون الكبير لنا لإخراجه بهذه الصورة.

الأساتذة عفاف مدني التي قدمت لنا المساعدة و بعض النصائح الهامة.

المستخلص

نظراً لما يشهده العالم من تطور في مجال الاتصالات وخاصة الانترنت أصبحت الحاجة ملحة إلى وجود طرق حماية للملفات التي يتم إرسالها من مكان إلى آخر ومن بين أساليب هذه الحماية ، برز علم الإخفاء الذي يتميز بنقل الرسائل عبر وسائط النقل (الملفات) دون ملاحظة عملية النقل هذه من قبل أي متطفل.

يقدم البحث فكرة مقترحة لإخفاء النصوص داخل الملف الصوتي من نوع ملف wav إذ يتم أولاً قراءة النص لاستخراج الرسالة المطلوب إخفاؤها ثم ضغط تلك الرسالة وإخفاؤها في ملف الصوت .

تم تطبيق الخوارزمية على أكثر من ملف صوتي وحققت نسبة استرجاع جيدة لبيانات الرسالة النصية ودون إحداث أي تشويه ملحوظ في الملف الصوتي مع إمكانية إستيعاب مختلف الأحجام من الملفات النصية.

ABSTRACT

The world is tends now a lot of development in communication field specially in internet, therefore it is very important to find security methods for files that is sent from one place to another.

One of these security approaches is steganography which have characteristic of transfer messages within transmission media (files) without notice from any obtrusive. This research provide a new algorithm for hiding text in audio file (wav file), first the text file will be read to extract the message which is hidden, this message will be compressed before hiding it inside sound media.

This algorithm was applied on more than one example and good results were obtained without missing the text message or notice any noise in the audio file with possibility to embed different sizes of text files.

شرح الاختصارات

المعنى باللغة الإنجليزية	الاختصار باللغة الإنجليزية
Least Significant Bit	LSB
Peak Signal To Noise Ratio	PNSR
Mean Squared Error	MSE
Human Auditory System	HAS
Pulse Code Modulation	PCM
Resource Interchange File Format	RIFF
Real Audio Media	RAM, RM, RA
Audio Interchange File Format	AIFF
Motion Picture Experts Group audio layer 3	MPEG
Lempel-Ziv-Welch	LZW
Run-length encoding	RLE

المصطلحات

المصطلح بالإنجليزية	شرح المصطلح
Steganography	انه فن وعلم إخفاء المعلومات (او الرسالة) باستخدام ملف حامل لها.
Cryptography	هو دراسة لطرق إرسال الرسالة بصورة أخرى لا يستطيع فك رموزها إلا المرسل والمستقبل.
Least Significant Bit	هي أبسط طريقة لإخفاء البيانات السرية في الوسائط. عن طريق استبدال ال bit اقصى اليمين في byte ملف الوسائط ب bit من الملف السري.
Lossless compression	هو أن يتم ضغط البيانات دون أن يتم فقد جزء منها.
Lossy Compression	في هذه الطريقة عملية الضغط قد يصاحبها فقدان في البيانات المضغوطة
Java	لغة برمجة .
MATLAB	بيئة عمل تحتوي على مجموعة من لغات البرمجة
Phase coding	طريقة إخفاء في الملفات الصوتية تعتمد على دمج الرسالة بشكل Bits في مواضع انقلاب الطور بالموجة الصوتية.
SPREAD SPECTRUM	طريقة إخفاء في الملفات الصوتية تعتمد هذه الطريقة على نشر موجات ضمن نطاق واسع من الترددات لا يمكن تمييزها عن الضوضاء (Noise) وتحتوي بداخلها على البيانات المراد ارسالها.
ECHO HIDING	تقوم هذه الطريقة على توليد صدى للصوت بمسافة زمنية قصيرة غير ملحوظة من الاذن البشرية بين الصوتين ويتم التشفير بواسطة اختلاف المسافات الزمنية بين الصدى والصوت الاصلي.
Wav,MP3,RM,RA,M,AIFF	إمتدادات الملفات الصوتية.
Huffman Coding	طريقة لضغط الملفات تعتمد علي تكوين شجرة من الملف المراد ضغطه.
Run-length encoding	هو نموذج بسيط جدا من عمليات ضغط البيانات ، يتم تخزين القيمة المكررة على شكل قيمة بيانات واحدة بجانبها عدد مرات التكرار
LZ77	تقوم هذه الخوارزمية باستبدال العناصر المكررة في البيانات بالاشارة اليها في شكل زوج من الارقام.
LZW	خوارزمية مشهورة لضغط البيانات بدون ضياع أي جزء منها تم إنشاؤها من قبل أبراهام ليميل ,جاكوب زيف ,وتيري فيلش.
PSNR	عبارة عن مصطلح هندسي للنسبة بين اعلى درجة للإشارة و الضوضاء التي تؤثر على دقة الإشارة.
MSE	هي معادلة لقياس متوسط مربعات الأخطاء في العينة المستخدمة .

فهرس الأشكال

ص	اسم الشكل	رقم الشكل
2	يوضح تدرج التقنيات المستخدمة في المشروع	1.1
6	يوضح طرق الإخفاء وأنواع الإخفاء في الملفات الصوتية	1.1.2
10	يوضح طريقة تنفيذ خوارزمية ال LSB 1 .	2.1.2
11	يوضح طريقة تنفيذ خوارزمية ال LSB 2 .	3.1.2
11	يوضح طريقة تنفيذ خوارزمية ال LSB 3 .	4.1.2
12	يوضح طريقة تنفيذ خوارزمية ال LSB 4 .	5.1.2
13	يوضح المخطط الإنسيابي لطريقة عمل الخوارزمية المقترحة	6.1.2
14	يوضح المخطط الإنسيابي لطريقة عمل الخوارزمية المقترحة	7.1.2
16	يوضح المقاطع المتداخلة لملف الصوت من نوع RIFF	8.1.2
19	يوضح أنواع ضغط البيانات	9.1.2
21	يوضح شجرة ترميز هوفمان	10.1.2
22	يوضح مسار علمية الإسختراج في ترميز هوفمان	11.1.2
26	الشكل 1.3 يوضح كيفية إجراء عملية التضمين	1.3
26	الشكل 2.3 يوضح الرسالة التي تظهر بعد عملية التضمين	2.3
27	الشكل 3.3 يوضح كيفية إجراء عملية الإسختراج	3.3
27	الشكل 4.3 يوضح الرسالة التي تظهر بعد عملية الإسختراج	4.3
36	يوضح نتائج ال PSNR لخوارزمية ال LSB 1 بدون ضغط للبيانات	1.4
36	يوضح نتائج ال PSNR لخوارزمية ال LSB 1 مع ضغط للبيانات	2.4
37	يوضح نتائج ال MSE لخوارزمية ال LSB 1 بدون ضغط للبيانات	3.4
37	يوضح نتائج ال MSE لخوارزمية ال LSB 1 مع ضغط للبيانات	4.4

37	يوضح نتائج ال PSNR لخوارزمية 2 LSB بدون ضغط للبيانات	5.4
37	يوضح نتائج ال PSNR لخوارزمية 2 LSB مع ضغط للبيانات	6.4
38	يوضح نتائج ال MSE لخوارزمية 2 LSB بدون ضغط للبيانات	7.4
38	يوضح نتائج ال MSE لخوارزمية 2 LSB مع ضغط للبيانات	8.4
38	يوضح نتائج ال PSNR لخوارزمية 3 LSB بدون ضغط للبيانات	9.4
39	يوضح نتائج ال PSNR لخوارزمية 3 LSB مع ضغط للبيانات	10.4
39	يوضح نتائج ال MSE لخوارزمية 3 LSB بدون ضغط للبيانات	11.4
39	يوضح نتائج ال MSE لخوارزمية 3 LSB مع ضغط للبيانات	12.4
39	يوضح نتائج ال PSNR لخوارزمية 4 LSB بدون ضغط للبيانات	13.4
40	يوضح نتائج ال PSNR لخوارزمية 4 LSB مع ضغط للبيانات	14.4
40	يوضح نتائج ال MSE لخوارزمية 4 LSB بدون ضغط للبيانات	15.4
40	يوضح نتائج ال MSE لخوارزمية 4 LSB مع ضغط للبيانات	16.4
40	يوضح نتائج ال PSNR الخوارزمية المقترحة مع ضغط للبيانات	17.4
41	يوضح نتائج ال PSNR الخوارزمية المقترحة بدون ضغط للبيانات	18.4
41	يوضح نتائج ال PSNR الخوارزمية المقترحة مع ضغط للبيانات	19.4
41	يوضح نتائج ال PSNR الخوارزمية المقترحة بدون ضغط للبيانات	20.4

فهرس الجداول

ص	إسم الجدول	رقم الجدول
17	يوضح معاني المصطلحات في الشكل 8.1.2	1.1.2
21	يوضح عدد تكرارات الحروف في كلمة Mississippi River	2.1.2
22	يوضح التشفير لكل حرف من حروف كلمة Mississippi River	3.1.2
28	يوضح أسماء الملفات الصوتية المستخدمة وأحجامه	1.2.3
28	يوضح أسماء الملفات الصوتية المستخدمة وأحجامها	2.2.3
31	يوضح نتائج ال PSNR لخوارزمية LSB 1	1.4
32	يوضح نتائج ال MSE لخوارزمية LSB 1	2.4
32	يوضح نتائج ال PSNR لخوارزمية LSB 2	3.4
33	يوضح نتائج ال MSE لخوارزمية LSB 2	4.4
33	يوضح نتائج ال PSNR لخوارزمية LSB 3	5.4
34	يوضح نتائج ال MSE لخوارزمية LSB 3	6.4
34	يوضح نتائج ال PSNR لخوارزمية LSB 4	7.4
35	يوضح نتائج ال MSE لخوارزمية LSB 4	8.4
35	يوضح نتائج ال PSNR للخوارزمية المقترحة	9.4
36	يوضح نتائج ال PSNR للخوارزمية المقترحة	10.4

فهرس المحتويات

رقم الصفحة	المحتوى
	الباب الأول
	المقدمة
1	1.1 المقدمة
2	2.1 حدود المشروع
3	3.1 مشكلة المشروع
3	4.1 أهداف المشروع
4	5.1 المنهجية المتبعة و الأدوات
4	6.1 تنظيم المشروع
	الباب الثاني
	الإطار النظري
	الفصل الأول:
5	1.1.2 المقدمة
5	2.1.2 مفاهيم أمن المعلومات
6	3.1.2 أساليب الإخفاء
8	4.1.2 الإخفاء في الصوت
9	5.1.2 أنواع الإخفاء في البت الأقل أهمية
10	6.1.2 الإخفاء في البت الأقل أهمية
15	7.1.2 أنواع الملفات الصوتية
15	8.1.2 ملف الصوت ذو الإمتداد wav
18	9.1.2 ضغط البيانات (Data compression)
20	10.1.2 خوارزمية هوفمان (Huffman Algorithm)
	الفصل الثاني:
23	1.2.2 المقدمة
13	2.2.2 الدراسات السابقة
	الباب الثالث
	تصميم النظام و التجارب
	الفصل الأول:
25	1.1.3 المقدمة

25	2.1.3 المنهجية المتبعة
25	3.1.3 تصميم النظام
	الفصل الثاني:
28	1.2.3 المقدمة
28	2.2.3 التجارب
	الباب الرابع النتائج
30	1.4 المقدمة
30	2.4 مقياس (PSNR)
31	3.4 مقياس (MSE)
31	4.4 النتائج
36	5.4 مخططات لتوضيح التباين في النتائج
	الباب الخامس التوصيات و المراجع
43	1.5 التوصيات
43	2.5 الخاتمة
	المراجع