INCREASING ROBUSTNESS OF DATA HIDING IN AUDIO SIGNALS

Hussein A. Lafta
Department of computer science, College of sciences for women, University of Babylon

1-Aim of the Search

In this search, we will first study the use of steganography with cryptography methods available for audio files, to increase the robustness of audio signals. Then we implement algorithm (low bit encoding) to hide a message, encrypted with a key, in an audio file, so that it can only be decoded using the same key (or public key cryptography methods can be used, i.e. public/private keys). We would be investigating the different audio formats (i.e. AU, WAV, AIFF, MP3) currently available for implementation.

2-Introduction

In an ideal world we would all be able to openly send encrypted email or files to each other. However there are often cases when this is not possible, steganography can come into play. If the u of cryptography is prohibits, we can send encrypted messages by hiding the encrypted message in another innocuous file using steganographic techniques.

Computer files (images, sound recordings, even disks) contain unused or insignificant areas of data. Steganography[2] takes advantages of these areas, replacing them with information (encrypted mail, for instance). The files can then be exchanged without anyone knowing what really lies inside them. Steganography can also be used to place a hidden "trademark" in mages, music, and software, a technique referred to as watermarking.

3-Coding a message in audio using low-bit method

Data hiding in audio signals is especially difficult since the humuii auditory system (HAS) operates over a wide dynamic range. However, while the HAS has a large dynamic range, it has a fairly small differential range. As a result, loud sounds tend to mask out qiiiet sounds. In our method, we will try to exploit these traits.

Low-bit encoding[1] is one way of embedding data into other data structures. By replacing the least significant bit of each sampling point by a coded binary string, we can encode a large amount of data in an audio signal. This method is useful only in closed, digital-to-digital environments.

4-Implementation

4-1 Audio File Forinat

The use of steganography techniques combined with encryption needs the data ... and file formats. A data format must including the following attributes: 1- ... technique
... channels
...
... per sample .

5-Frame rate
6-Frame size in bytes

A file format specifies the structure of a sound file, and is 'represented by an *Audio File Format* object, which contains: 1-The file type(WAVE, AU, AIFF, etc.)
2-The files, length in bytes
3-The length of the audio data contained in the file
4- An audioformat object that specifies the data format of the audio data contained in the file.

In implementation , we treat the AU file as 8-bit mu-law encoded.[5]

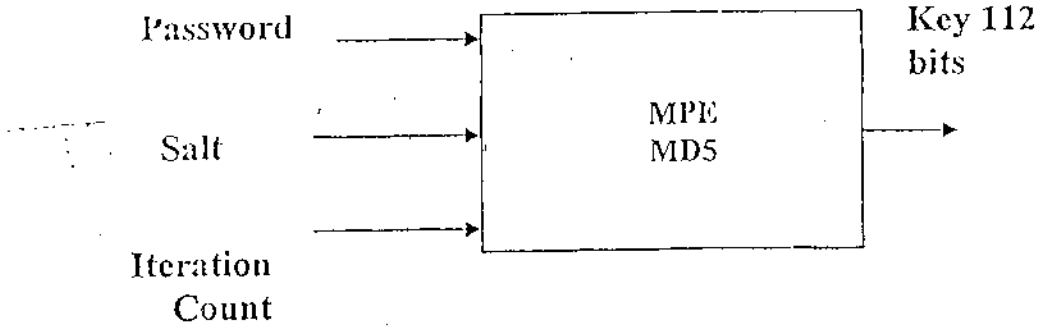
4-2 Encryption method used

A general approach to password-based cryptography is to combine a password with a salt to produce a key. The salt can be viewed as an index into a large set of keys derived from the password, and need not to be kept secret. So it is impossible to opponent to construct a table of' possible keys. An opponent will thus be limited to searching through password separately for each salt. We construct key derivation techniques that are expensive ,to increase the cost of exhaustive search, we include an iteration count in the key derivation technique

Salts and iterations count formed the basis for password-based encryption. A salt has served the purpose of producing a large set of keys corresponding to a given password, among which one is selected at random according to the salt. An individual key in the set is selected b applying a key derivation function KDF, as

DK=KDF(P,S)

Where DK is the derived key, P is the password, S is the salt as shown in the figure 1



Figure(1) Key Derivation Function

Encryption algorithm

One of the function defined in [,we chose PBKDF1, which employs a hash function ,in this case MD5.

PBKDF 1(P,S,c,dklen)
Options: Hash
Input : P,S,c,dklen
Where P is password
S is a salt
C is iteration count
Dklen is intended l of derived key
Output DK
Algorithm steps:

1- Select suitable length for dklen.
2 Apply hash function for c iterations to the concatenation of the password P and the salt S, then extract the first dklen to produce a derived key DK

T1 =Hash(p\\S),
T2=Hash(T1),
.....
.....
TC= Hash(Tc-1),
DK=Tc < 0..dkln-1>

3-Output the derived key DK. [4]
Steganalysis focuses on two aspect:
1 -Dedection of embedded message, and
2-Destruction of embedded message.

In the implementation the detection process is difficult since HAS has a fairly small differential range.

Our implementation is strong against attacks such(Host-stego attack, Stego-only attack) since the attacker is unaware of the encryption algorithm and also the parameters of the algorithm. There is no secure stegosystern if the attacker knows both host medium, arid stego medium. The encryption adds another level of security to the conventional stegosystem. It is necessary to maintain the same salt and iteration count
to generate the same key in both encryption and decryption process. This reduce the key space in a brute force attack. But the salt which is compiled with the source code itself, makes it harder to guess. Also the triple DES is regarded as a alternative to conventional DES. Thus the implementation shown in the block diagram form as in fig.2

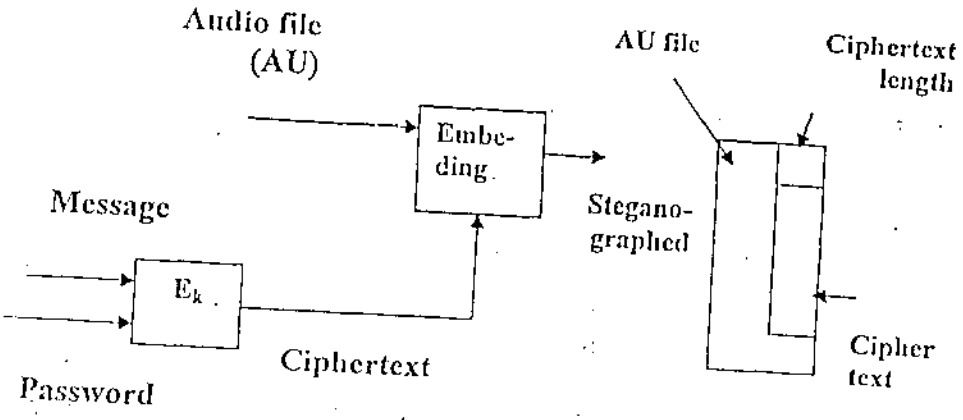


Fig.2 Block diagram of the proposed system

5-Conclusions and Future works

The major disadvantage of low-bit encoding, is poor immunity to manipulation. Encoded information can he destroyed by channel noise. resampling, etc., unless it is encoded with redundancy techniques. This method is useful in closed, digital environments. Other data hiding techniques such as phase encoding, spread spectrum, and echo hiding have better immunity to manipulation. The drawback of the implementation is the difficulty n the detection process because HAS has a fairly small differential range.

Examples of steganography attacks are: Stego-only attack, Host-stego attack, and chosen message attack. Our implementation is strong against these types of attacks since the attacker is unaware of the encryption. algorithm and also the parameters of the algorithm. The encryption adds another level of security to the conventional stegosystem.

Future Works

1-Provision of greater flexibility in terms of the algorithm used for encryption.
2-Provide option to use "phase Encoding", "Echo data hiding"
3-Support for different audio formats (WAV,AIFF).

7.References

[1] Bender W., Gruhl D., Morimoto N., Lu A., "Techniques for data hiding", IBM Systems Journal, Vol. 35, Nos 3&4, 1996.
[2] Java Sound API - http://java.sun.com/products/java medialsound/
[3] PKCS#5: Password-Based Encryption Standard. Version 2.0, RSA Laboratories March 1999.
[4] Java Cryptography Extension (JCE) – http://java.sun.com/products/jce/
[5] Declan McCullagh, "Bin Laden: Steganography Master?", Wired News Oct. 2001 (http://www.wired.com/news/politics/0, 1283,41 658,00.html)
[6] Homepage - http://bladeenc.mp3.no/

مجلة جامعة بابل / العلوم الصرفة والتطبيقية / المجلد ١٠/ العدد ٣ : ٢٠٠٥

زيادة قوة امكانية اخفاء المعلومات في الاشارة الصوتية

الخلاصة

تدرس في هذا البحث اولاً كيفية استخدام الستكانو مع طرق التشفير المتوفرة لملفات الصوت، لغرض زيادة قوة اشارات الصوت. تم بعد ذلك تنفيذ خوارزمية (خوارزمية تشفير البت المنخفضة) لاخفاء الرسالة المشفرة مع مفتاح. في ملف صوت ما ممكن فقط حل الشفرة باستخدام المفتاح (او مفتاح عام).

تم استعراض صيغ الصوت المختلفة مثل (AU, WAV, AIFF, MP3 ...الخ) المتوفرة حالياً لاغراض التنفيذ.