Encrypted Image Watermark in Audio Files Using Homogenous Deffie-Hellman with Chebyshev Polynomial

Dr. Hala B. Abdul Wahab
Computer Science Department, University of Technology/ Baghdad
Email:uot_techmagaz@yahoo.com
Dr. Abdul-Mohssen J. Abdul-Hossen
Computer Science Department, University of Technology/ Baghdad
Sana Ahmed Kadhom
Computer Science Department, Al Mammon University College/Baghdad

Received on:20/6/2016 & Accepted on:24/11/2016

ABSTRACT

Due to the expanding utilization of advanced media, the assurance of protected innovation rights issue has turned into an essential issue. Digital watermarking is currently drawing consideration as another technique for shielding media content from unapproved duplicating. In this paper, watermarking image (logo) will be encrypted using a key constructed by a proposed homogenous method of Diffie-Hellman and chebyshev polynomial. The encrypted watermark will be embedded in different samples from the transformed file (DCT) of audio. The embedding process will depend on binary similarity between the audio and watermark bits which reduces the effect of embedded data. The proposed method for the key generation is more secure and complicated since it combines the strength factors of both Diffie-Hellman and Chebyshev polynomial. The effect of the embedding is nonperceptibile and nondetectable.

Keywords: watermark, audio, Diffie-Hellman, Chebyshev polynomial, DCT.

INTRODUCTION

Cyber security is the assurance from a digital criminal exercises, including burglary, change, bending and unapproved utilization of digital media; When imperative message is to be transmitted in the net, the message ought to be ensured by scrambling or concealing it before transmission.[1]

Digital watermarking is the procedure of embedding critical data inside a media such that the receiver can check the received information. Sound watermarking has been demonstrated as a standout amongst the most important advanced technique for ensuring sound files against any adjusting process.[2]

In the earlier decade, a lot of work has been done to scramble audio watermarking using different strategies of cryptosystems and hiding methods. Diffie-Hellman is one of the most important method used for key exchange, a key to be used for encrypting and decrypting any message before transmission between parties.[3] Chebyshev polynomial is proved to be a chaotic producer function which is used widely in security processes.[4]

Hooman and Sina[5], proposed a method for embedding watermark picture in audio by segmenting the picture into segments and each segment into sections, these sections will transformed using DCT and a synchronization code will be added then retransformed, scrambled and hidden in audio.

Wang, Niu and Lu[6], proposed a digital audio watermark using wavelet moment invariance. It divides the audio signal into two sections, the first will hold the synchronization code and the second will be transformed to 2D and hidden as watermark. Xinkai W., Pengjun W., Peng Z.,

https://doi.org/10.30684/etj.34.6B.18
2412-0758/University of Technology-Iraq, Baghdad, Iraq

Shuzheng Xu and Huazhong Y.[7], sujested a method where a binary image encrypted by Arnold transform as watermark is embedded in the vector norm of the segmented approximation components, the count of which depends on the size of the watermark image, after DWT of the original audio signal through quantization index modulation (QIM) with an adaptive quantization step selection scheme.

In this paper a new method is proposed to produce an encryption key using Diffie-Hellman algorithm with a modification in the process of calculating the secrete individual numbers by using chaotic chebyshev polynomial to produce that key. The proposed algorithm combines the strength factors of both methods; It reserve the power of exponential of Diffie-Hellman but with variant exponents depending on the power of chaotic Chebyshev polynomial.

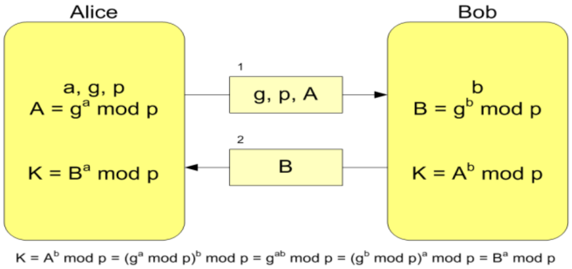
DCT (discrete cosine transform) has been used frequently with audio files, it concentrate the energy of the signal in the first few values while the rest of values have less magnitude.[8] In this paper, DCT applied on sub parts of the audio called frames, each part has a small number of samples (256 sample) to make the embedding process had the minimum effect on the audio with an expansive spread range..

The paper has many sections, the first section for Diffie-Hellman, the second for chebyshev polynomial and the third for the proposed algorithm.

I. Cryptographic Explanation of Classical Diffie-Hellman algorithm:

Diffie–Hellman key exchange is a particular strategy for safely exchanging cryptographic keys over an open channel and was one of the main open key conventions. The original implementation of the protocol uses the multiplicative group of integers modulo p, where p is prime, and g is a primitive root modulo p. These two values are chosen in this way to ensure that the resulting shared secret can take on any value from 1 to p–1.[9] Here is an example of the protocol

1. Alice and Bob agree on a public number g and a prime number p.
2. Alice chose a random number a, where $1 \leq a < n$.
3. Bob chose a random number b, which is also $1 \leq b < n$.
4. Both sides find their corresponding calculated number and send to the other side.
5. Both sides can now calculate the secrete key.


Alice
Bob
a, g, p
A = g^a mod p
K = B^a mod p
1
g, p, A
2
B
b
B = g^b mod p
K = A^b mod p
K = A^b mod p = (g^a mod p)^b mod p = g^ab mod p = (g^b mod p)^a mod p = B^a mod p

Diffie-Hellman key exchange process

II. Explanation of Chebyshev Polynomial

Chebyshev polynomial is one of a great importance in mathematic especially in approximation theory, it is defined on [-1, 1]. Chebyshev polynomial has known as a main of chaotic dynamic for long time, it defined on finite field.[4]

Definition: Let $T(N) : \{0;1;N - 1\} \rightarrow \{0;1; N -1\}$ is a self-mapping, the extended Chebyshev Tn(x) is defined as:

$$T_0(x) = 1 \bmod N$$
$$T_1(x) = x \bmod N$$
$$T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x) \bmod N$$

Where $x \in \{0; 1; 2; \cdot \cdot \cdot N - 1\}$ and N is a prime.

III. The Proposed Algorithm

The proposed algorithm has many steps, the first is for creating and exchanging the encryption-decryption key and this is done by the following:

First: (Party1 side)

Step one (key generating and exchange):

1- Party1 and Part2 chose g and q which are primitive large numbers.
2- Party1 chose x_a, which is his private key
3- Party1 compute Y_a, where:
   $Y_a = Tx_a(g) \bmod q$, where T is chebyshev polynomial.
4- Party1 send Y_a to Party2
5- Party2 compute key K by:
   $K = Tx_b(Y_a) \bmod q$
6- Party1 compute K using received Y_b.

Step two (logo processing):

1- Read logo image.
2- Encrypt the image data using key K.
3- Convert to binary.

Step three (Hiding logo into audio):

1- Read audio file.
2- Divide the audio file to sub parts each of 256 sample(power 2).
3- Convert each sub part to DCT.
4- Convert DCT to binary.
5- In the first 10 binary samples only, replace the LSB of each sample with the value of the logo binary data
6- Repeat 3-5 to each sub part.
7- Apply IDCT.
8- Send the audio file to Party2.

Second: (Party2 side)

Extraction process

1- Read the received audio file
2- Divide it into sub parts each of 256 samples.
3- Apply DCT on each part.
4- Convert to binary.
5- Read the LSB from each binary sample.
6- Convert the resulting bits to decimal.
7- Decrypt using key K.
8- Verify the logo.

Key generation and exchange using proposed algorithm:

Let g=2, q= 11;
Party1: $x_a = 3$, then
$T_3(x) = 4x^3 - 3x \bmod q$; (chebyshev)
$Ya = Tx_a(g) \bmod q$
$= 4x^3 - 3x \bmod 11$
$= 4(2^3) - (3*2) \bmod 11$

$=4$

Send Y_a to Party2

Party2: $x_b=2$, received Ya, then

$T_2(x) = 2x^2 – 1 \bmod q$; (chebyshev)

$K = Tx_b(Ya) \bmod q$

$= T_2(4) \bmod 11$

$= 2*(4^2) – 1 \bmod 11$

$K_b = 9$

$Y_b=Tx_b(g) \bmod q$

$=2x^2 -1 \bmod q$

$=2(2^2) – 1 \bmod 11$

$=7$

Send Y_b to Party1;

Party1: received Y_b from Party2;

$K= T_{xa}(Y_b) \bmod q$

$= T_3(7) \bmod q$

$= 4(7^3) – 3*7 \bmod 11$

$K_a = 9$

That key and multiplicative algorithm will be used to encrypt and decrypt the logo image.

Results and Evaluations

Logo image in figure 1 was used as a watermark to be hidden in the audio file.

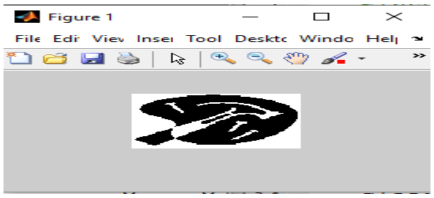


Figure 1

That image encrypted with the key exchanged (as shown in figure2).

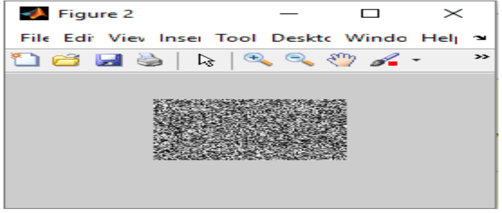


Figure 2

Then embedded in the audio file in Figure 3 (plot of the original audio file (.wav));

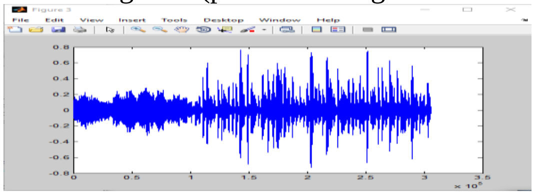


Figure 3

The watermarked audio file in figure 4 (plot of the watermarked audio file) was sent to the receiver.

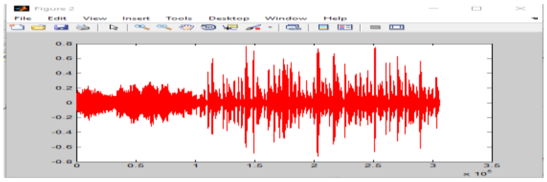


Figure 4

The watermark is nonperceptible to HAS (Human Auditory System), because the watermark had no effect on the audibility of the sound; it also nondetectable since the logo bits were spread on a wide range of audio signal, it didn't add or remove data to the audio file, only tiny change to values defused in audio. The algorithm security depends not only on spreading watermark on wide area of audio, but also on encrypting the logo using key generated and distributed with a complex algorithm and polynomial.

The bit error rate test, which is used to find the ratio of changed bits according to the number of watermark image bits:

$$\text{BER (\%)} = (E/T) * 100\% \qquad \ldots\ldots\ldots (1)$$

E: is the number of watermark bits that not match the replacement bits of audio file;

T: the total number of bits in watermark; [10]

This test find the number of audio bits that were changed when the watermark added, the ratio is find corresponding to the total number of WM data.

$$\text{SNR=Noise (WM)/Signal (audio data) *100\%} \qquad \ldots\ldots\ldots.. (2)$$

This test finds the number of audio bits that were changed when the watermark added, the ratio is found corresponding to the total number of audio data.

For a watermark image of size (60776 bit), the results were:

Audio-L	Missed	SNR%	BER%
19593344	30649	0.16	50.43
83396480	30500	0.04	50.18
140753920	30182	0.02	49.66
123239424	30467	0.02	50.13
63093760	30397	0.05	50.01
84672000	31460	0.04	51.76
83841280	30411	0.04	50.04

For the same audio files with a watermark image of size(18920 bit), the results were:

Audio-L	Missed	SNR %	BER %
19593344	9431	0.05	49.85
83396480	9438	0.01	49.88
140753920	9502	0.01	50.22
123239424	9486	0.01	50.14
63093760	9469	0.02	50.05
84672000	10415	0.01	55.05
83841280	9553	0.01	50.49

All results indicate that the watermark had very tiny effect on the signal; the SNR in all cases were minimums which record no effect on audio files. The BRE recorded values near half which means in each case the real embedded bits were half the size of the watermark data and that's because the proposed method took an advantage of the binary similarity between the audio file and the watermark data.

From previous results, the method was proved to be effective by having the minimum effect on the audio signals which means, the proposed method had preserve the quality of the original audio signal, nonpersceptabile and nondetectable which are the major characteristics of any audio watermarking method.

CONCLUSIONS

In this paper, the used technique spread the signal watermark in frequency spectrum. The watermark was encrypted so that even if altered during transmission, no one can decrypt the logo image unless has the secret key. The strength of key generating algorithm has improved by using the chaotic characteristics of chebyshev polynomial to the strength of well known Diffie-Hellman algorithm. The embedded data were always near half because of binary similarity, which reduces the effect of the embedding process. The proposed algorithm had passed many types of test with good results.

REFERENCES

[1]Agbaje, M.O, Awodele O., and Ogbonna A.C, "Applications of Digital Watermarking to Cyber Security (Cyber Watermarking), 2015, Proceedings of Informing Science & IT Education Conference (InSITE).

[2]Juergen Seitz ,Digital watermarking for digital media",2005, InfoSCI.

[3]Garzia, F. (2013), Handbook of Communications Security, public key exchange, WIT Press, p. 182, ISBN 1845647688

[4]Wang Dahu and Wei Xueye, "Applying Extended Chebyshev Polynomials to Construct a Trap-Door One-Way Function in Real Field",IEEE, 2009 ,First International Conference on Information Science and Engineering.

[5]Hooman N. and Sina T.," A New Approach to Audio Watermarking Using Discrete Wavelet and Cosine Transforms", 2010, 1st international conference on communications engineering, University of Sistan & Baluchestan.

[6]Wang Xiang-yang, Niu Pan-pan, Lu Ming-yu, A robust digital audio watermarking scheme using wavelet moment invariance, The Journal of Systems and Software, 2011, Volume 84 Issue 8, pp. 1408-1421.

[7]Xinkai Wang, Pengjun Wang, Peng Zhang, Shuzheng Xu, Huazhong Yang, A norm-space, adaptive, and blind audio watermarking algorithm by discrete wavelet transform, Signal Processing, April 2013, Volume 93, Issue 4, pp. 913–922.

[8]Syed Ali Khayam, "The Discrete Cosine Transform (DCT), Theory and Application", 2003, Department of Electrical & Computer Engineering, Michigan State University

[9]Garzia, F.," Handbook of Communications Security", WIT Press, 2013, p. 182,ISBN 1845647688.

[10]Shilpa Arora, Sabu Emmanuel, "Real-time adaptive speech watermarking scheme for mobile applications", ICICS-PCM, 2003, Singapore.

[11]S. Shokri, M. Ismail, N. Zainal, A. Shokri, "BER Performance of Audio Watermarking using Spread Spectrum Technique", The 4th International Conference on Electrical Engineering and Informatics (ICEEI 2013).

[12]M. Zhao, J-S Pan, S.Tsung Chen, "Optimal SNR of Audio Watermarking by Wavelet and Compact PSO Methods", Journal of Information Hiding and Multimedia Signal Processing, Volume 6, Number 5, September 2015.

[13]Abhijeet Kotwal, Prof.K.N.Shedge, A Review on "Hide the data in Encrypted video using Private Key for secure Transmission", International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 12, December 2015.

[14]Abdul Monem S.Rahma, Abdul Mohssen J.Abdul Hossen & OmarA.Dawood, "Public Key Cipher with Signature Based on Diffie-Hellman and the Magic Square Problem", Engineering & Technology Journal, 2016, V34, No. 1.

[15]Yossra Hussain Ail & Zahraa A.H. Alobaidy, "Images Encryption Using Chaos and Random Generation", Engineering & Technology Journal, 2016, V34, No. 1.