ISSN: 0067-2904

Advanced Password Authentication Protection by Hybrid Cryptography & Audio Steganography

Eman Salim Ibrahim Harba
Computer and Internet Unit, College of Arts , University of Baghdad, Baghdad, Iraq.

Abstract

Data transmission in public communication system is not safe since of interception and improper manipulation by attacker. So, the attractive solution for these problems is to design high secure system that reduce the ability of attacker from getting sensitive information such as (account ID, passwords, etc.). The best way is combine two high secure techniques: steganography technique, which is the method of hiding any secret information like data, password and image behind any cover file and cryptography, which is convert the data to unreadable data. This paper suggests a crypto-stego authentication method to provide a highly secured authentication. The proposed method is utilized audio steganography and AES Cryptography. The authentication key (password) is spilt to two parts, the first half is used as input text to stego-crypto process while the second half used as crypto key. The crypto key is encrypted using HMAC-SHA256 hash algorithm and sent to server while the second half has encrypted with AES that ciphered with random xor cipher algorithm then embedding in wave audio by used Least Significant Bit (LSB) algorithm then streamed to server. This method can trick the attacker to focused on hashed value that appears with streaming data while the part of key hided within the cover file.

Keywords: Password Authentication, Cryptography, Steganography, AES, Audio Steganography.

حماية كلمة سر الدخول المتقدمة بالاعتماد على دمج تقنيتي التشفير والأخفاء بالصوت

إيمان سليم ابراهيم حربة
وحدة الحاسبة والإنترنت، كلية الاداب، جامعة بغداد، بغداد، العراق.

الخلاصة

ان نقل البيانات في أنظمة الاتصالات العامة تعتبر غير أمنه بسبب إمكانية اعتراض البيانات والتلاعب بها من قبل المهاجم. لذا فان الحل العملي لهذه المشاكل هو عن طريق تصميم نظام عالي الأمان الذي يقلل فرص المهاجم على الاستيلاء على المعلومات الحساسة (مثل أسماء الحسابات، كلمات السر، وغيرها). أن أفضل طريقة هي بدمج تقنيتين عالية الأمان هما: تقنية إخفاء المعلومات (Steganography) والتي هي طريقة إخفاء أي معلومات مهمه مثل البيانات، كلمات السر والصور ضمن أي ملف إخفاء، وتقنية التشفير (Cryptography) التي تحول البيانات الى بيانات مشفرة غير ممكن قرأتها. هذه المقالة تقترح طريقة تشفير- أخفاء في عملية التصريح للدخول لمواقع الويب. الطريقة المقترحة تستخدم الأخفاء بالصوت مع معيار التشفير المُطَور (AES). ان مفتاح الدخول (كلمة السر) ستقسم الى قسمين: القسم الأول سيستخدم كمدخل نصي الى عملية التشفير والاخفاء بينما النصف الثاني سيكون مفتاح التشفير. أن مفتاح التشفير سيتم تشفيره باستخدام

Email: emanharba_1212@yahoo.com

تقنية ب (HMAC) بخوارزمية التجزئة (256SHA) ومن ثم يتم ارساله للخادم، بينما الجزء الثاني سيتم تشفيره بخوارزمية معيار التشفير المُطَور (AES) التي تشفر مع خوارزمية XOR للشفرات العشوائية ومن ثم سيتم تضمينها في ملف صوتي نوع (wave) من خلال استخدام خوارزمية البتات قليلة الأهمية (Least Significant Bit) ومن ثم ارسالها الى الخادم. أن هذه الطريقة ستمكن من خداع المهاجم بحيث تجعله يركز على شفرات التجزئة التي تظهر مع البيانات المرسلة والتي هي فقط نصف المفتاح بينما النصف الأخر سيكون مخفي في ملف الأخفاء.

1. Introduction

Data security is a method of securing data from viewing by unauthorized users or scammers as well as offering high security to protect informations from modification. This field of data protection has got more attention through the recent years because of the large increase in data transfer rate across the internet. Thus, in order to increase the security aspects for data transfers throughout the internet, various techniques have been designed such as: digital watermarking, Cryptography, and Steganography. Steganography gives extra security by concealed the cipher text into a relatively invisible text, image, video or other formats. Steganography, is the art of concealing and transferring data throughout apparently innocuous carriers to hide the presence of data”. The visibility level is reduced using different hiding techniques. Steganography techniques can be implemented on various file formats such as audio (mp3, wmv, etc.), video (mpeg, dat, etc.) and images (jpeg, bmp, etc.). The embedded or hidden covers (text, audio, image, or video files) act as carriers to transmit the secret messages to the destination become withot any security breach. Cryptography is the technique that used to obtain security via encoding the data to convert them into non-readable forms so that not authorized users are not able to gain access to it. [1, 2].

Steganography is different from cryptography in the point that cryptography is works on keeping the message contents in secret, while steganography works on keeping the presence of a message secret. Both techiques are the ways to protect data from unwanted parties, however, neither of them alone is optimal and can be attacked. As the existence of hidden information is discovered or even suspected, the functionality of steganography is mostly defeated. The steganography strength should be increased by hybridizing it with cryptography [3]. This paper has been utilized a technique to hiding the encrypted antiunification data with an audio file (wave).

In audio steganography, the visibility of quality or clarity of audio file is not getting affected by the hacker, the audio file only going to be noticed when previewed and there is no trace of the hidden info. when stego file is opened, the information still not going to be noticeable because the information is placed in an encryption form that is also binary. As a result, it makes difficult for the enclosure to distinguish the imbedded data from the cover file. The approach that commonly used to concealing data inside Audio files is the low bit encoding which is relatively identical to Least Significant Bit(LSB) that is generally used in Images. LSB is one of the earliest and simpler technique utilized for hiding data within the digital audio (as well as other media types). Typically, LSB is based upon placing each bit from the message within the LSB of binary sequence of every sample (coefficient) of digitized audio file cover. [4].

In this paper a combination method of cryptography and steganography scheme is proposed for secure authentication key. They The key is split into: one to encrypted by HMAC hash and send to server and second encrypted by AES and then embedded within audio cover file. The cover file in use is a digital audio file. The sender hided the secret bits inside the cover audio file by using location selection within the coefficient, to create a stego-audio-file, so the malicious user is not able to detect the presence of the hidden key. At the server side, the server will check first the first hah key value to compered with stored key after passed this process then requested first half key that stored in database, then it will extract the hidden secret bits (encrypted Key) from the chosen position throughout the coefficient of stego-audio.

2. Previous Works

Yang and Wen (2008) [5], designed a novel encryption/decryption method using LSB algorithm and utilized public key cryptography, public key infrastructure, and watermark techniques by preserving integrity by using forensic imaging strategy. The computer forensic approach is applying to locate the parameter like PSNR, height and width of data, frame number, histogram of secrete message information after and before concealing to audio-video. In cases where all of these parameters are confirmed and determined to be correct, then it will transmit to receiver in contrast, if it not confirmed then it will stop the secrete message information in computer forensic block. Asad M et al. (2011) [6], proposed a audio steganography with an encrypted audio file using Advanced Encryption Standard(AES). Fatiha et al [7], examines the several audio steganography techniques such as phase coding, parity hiding, echo hiding and their comparison.

Sathya et al (2012) [8], proposed the powerful method of hidden text, audio, image and video. They present an effective method for concealing the data from hackers and it will transfer to the receiver in a secure way. In same year, Guizani and Nasser [9], explain many approach of audio steganography and LSB approaches with ORing technique found to be more secured.

Pathak and Nag. (2014) [10], analyzes LSB audio steganography with location identification and it gives good robustness and audio quality. Indrayani et al (2016), suggested a approach that enhance the security of data transfer by hybridizing cryptography and steganography. Mp3 file is used as the cover media and the secret message is encrypted by using AES algorithm applying a key that has been prepared by MD5 hash function. The secret message was imbeded in the homogeneous frame in mp3 files with addition of a key code.

3. Stego-Crypto Background

3.1 Overview of Audio Steganography by used Least Significant Bit Method

This method is one of the first methods that utilized for hiding information. Generally, it is dependent on embedding every bit from the message in the least significant bit (LSB) of the audio cover in a deterministic strategy. Therefore, for a 16 kHz sampled audio, 16kbps of data are concealed. The LSB technique will allow large embedding capacity for info and is fairly easy to apply or to merge with other hiding techniques. Even so, this technique is categorized by low robustness to noise insertion which usually reduces its security efficiency as it becomes susceptible even to simple attacks [7].

For example, the letter 'أ' has an ASCII code of 1571 (decimal), which is 1101100010100011 in binary. It will need sixteen consecutive bytes of audio data to store an 'أ': As an example, if the audio bytes before the insertion are [11]:

10000000.10100100.10110101,
10110101.11110011.10110111,
11100111.10110011.00110011

Then if need to add character like “A” of binary values “**1000001”**, then the audio bytes after the insertion are will be:

1000000**1**.10100100.1011010**0**,
1011010**0**.1111001**0**.1011011**0**,
1110011**0**.10110011.00110011

Where the bold are the ones that were modified by the transformation were bits are selected randomly.

3.2 Integration of Cryptography with Steganography

Cryptography is the method of change data into a scrambled code that can sent across a private or public network without concerning from stolen by hacker because it need the authorized key. Cryptography takes advantage of two main forms or styles of encrypting data; asymmetrical and symmetrical. The symmetrical encryptions use the exact key for encryption and in decryption. Symmetric cryptography is sensitive to linear cryptanalysis and plain text attacks, so this means that they are hackable and need times to decode [12].

AES is the wide-spread algorithm that has been authorized for use in encrypting standard material marked ‘SECRET’ by 128bit, 192bit and 256bit keys and designed for usage in encrypting official material marked ‘TOP SECRET’ with 192bit and 256bit keys through the Committee on National Security Systems of United States (CNSS). A quantity of AES parameters be based upon the key length. For example, if made use the key of size 128bit then the amount of rounds is 10 rounds, while it is 12 rounds for 192bit and 14 rounds for 256bits. The most wide-spread key size most likely to be used is the 128bit key [13].

The method of combined steganography with cryptography is a part of two steps [14]: encryption step, in which the secret data will be encrypting, and the stego step that the encrypted data will be encoding (imbedding inside cover). Initially, the secret info was encrypted by using AES. The encryption process result will then have embedded into a cover media by using the encoding process. In audio steganography, the encoding process is hiding the secret information on a homogeneous frame coming from an audio cover file. For decoding process, the message extraction will be done by reverse process of encoding; the process wherever each and every byte of info was gathered, following the decoding process, the message gathered will be decrypted by using same encrypted key to get the original secret data. The encryption key that used in encryption and decryption process is processed using hash function.

4. Proposed Method

The proposed method is based on trick attacker from getting authentication key by sending two keys by two different method, the actual authentication key is encrypted by use AES algorithm then hide within wave file by used audio steganography, while the key used in encryption will be hashed with HMAC SHA-256 hash function and sent to receiver. The process used half of key as input text wile used the remaining as encryption key. Soby this, the attacker will be trike by see the hash value and think it is the authentication key, while it is actually the crypto key, on other hand the authentication key will transfer securely with audio stream file. Figure-1 illustrated the scheme of overall process.

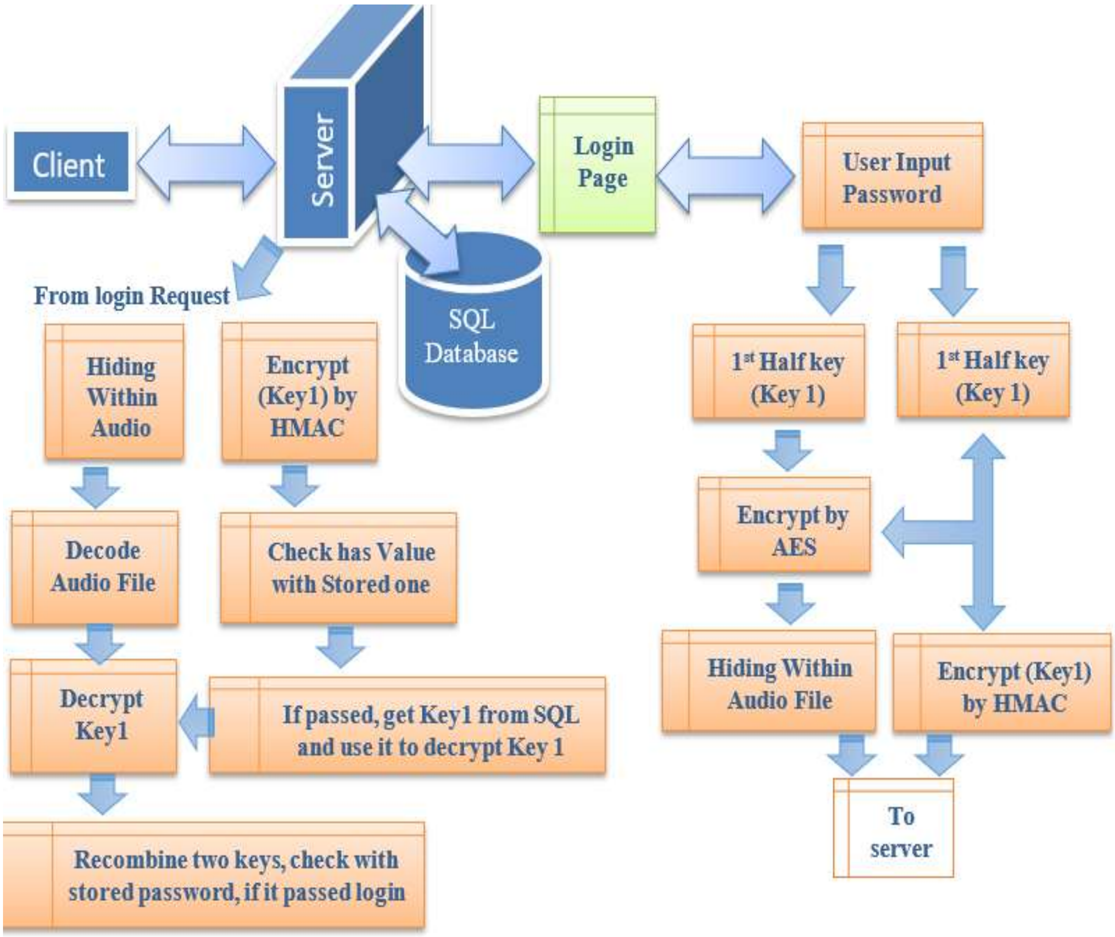


Figure (1): Proposed system processes

First of all, the split to two halves, the first treat as a secret data that was encrypted using AES while the encryption key was processed first using SHA256 hash function. The result of encryption process was then embedded into a cover media using the encoding process. Encoding process is an embedding process of a secret data on a homogeneous frame from a wave cover file. The cover is restively small size wave file that are randomly selected from database then stream back to server, also the server will continue streaming audio file randomly. After that, key extraction was done by decoding process as the opposite process of encoding; the process where every byte of information was gathered. From the result of decoding process, the key gathered was decrypted to obtain the real authentication key.

Client-Side Algorithm

Input:	Login Authentication (UserName, Password)
Output:	Hash Key and audio streaming wave file

Step 1: Start.

Step 2: Client is browsing pages in non-authenticated mode.

Step 3: Server is serving pages in non-authenticated mode, offering a small login option on each page Client sends Authentication Request identifying (UserName and password), only "UserName" send first to sever to identify:

- If an analog "UserName" was in database, the server sends back to page requesting "password" (Step 4).
- If UserName is not known, the Server will send back a message that user is not registered member.

Step 4: Key will pass to word counter, calculate the number of characters then pass to Check Tool, if it even divides on 2 and the number of character of key are same in both, if odd then the number of word subtract from 1 then dived by 2, the number of character of first part will be the same division result while the second part will be the division result plus one.

Step 5: The first half of key characters will be pass to crypto-stego process, while the second half of key characters have used as crypto key then hashed and transfer to server side. The both steps are:

A. Encrypt the crypto key (Key1) with SHA256 HMAC algorithm

1- Get the key value Key1 (which is the second half of key) and public key from server
2- Compute the hash of the input file by requested (HMAC SHA-256) algorithm from C# cryptography library
3- Reset in Stream to the beginning of the file.
4- Write the computed hash value to the output file.
5- Copy the contents of the source-File to the destination-File
6- Read from the wrapping Crypto-Stream
7- Send to server

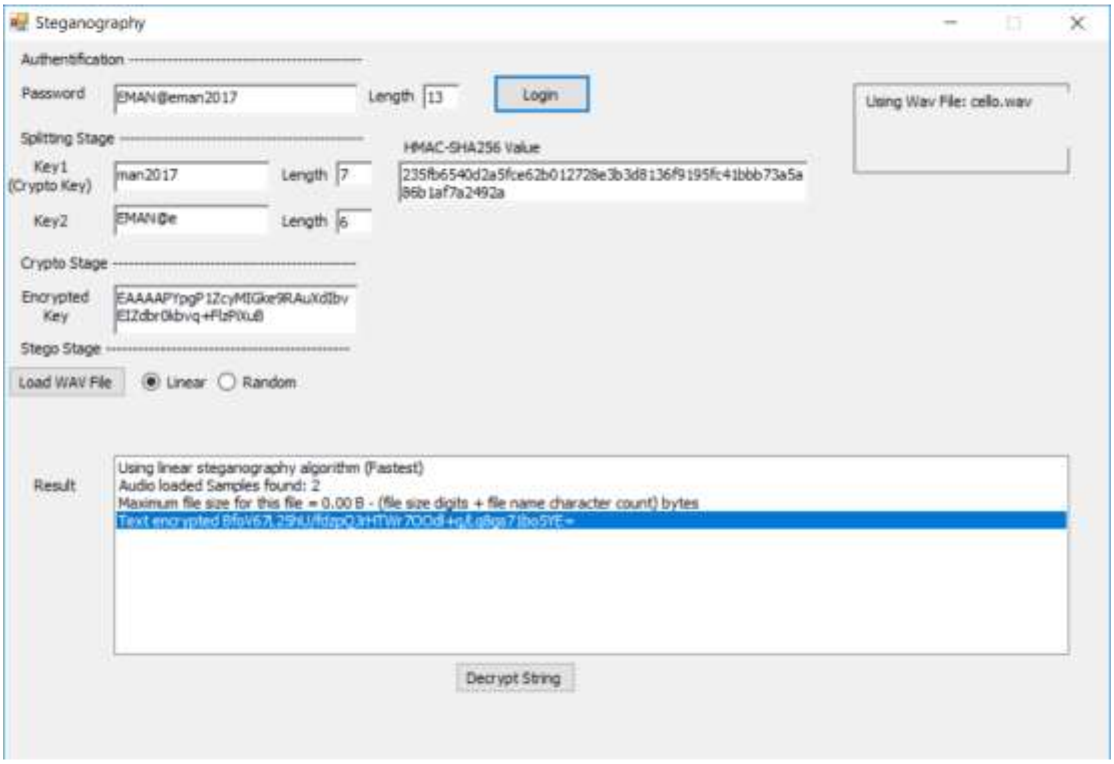
B. Encrypt the Key2 with AES and Key1

1- Initially the Key1 (Crypto Key), Key2 (the first half of key) and cover audio (wave file) are taken as input at the sender's side.
2- The Key2 is encrypted using AES algorithm using 256bit key by using (Key1).
3- The encrypted Key is embedded inside the cover audio using LSB technique.
4- After embedding the hash code of the samples of cover audio is produced using MD5 hash algorithm.
5- The hash code is embedded inside the cover audio and the stego audio is produced.
6- The stego audio file is sent to server

In server side, the processes done in opposite, as the client side sending authentication to server, the server have received both hash vale and streaming audio, the it will check the hash value is it identical, if it identical, bring Key1 value that stored in SQL server in registration process. In same time the server will analyses each wave file streams back from client to be decoded using same encoding algorithm and used Key1 to decrepit the result, if the wave file has a decrypt key then the server will get this part of key (Key 2) and recombed it with first key (Key 1) then used it to check the authentication process if it passes, the user will login, if not the server will be showing message to client to input the username and password again.

5. Experimental Test and Results

The proposed system has been designed with C#, the system simulates authentication process, the login password used is "EMAN@eman201" which is long password with upper lower characters with Symbols. The private key for HMAC is "mkf2u8121979". The stego cover used is small size wave file (~ 50 KB), the test result shown in Figure-2.



Authentification

Password: EMAN@eman2017 Length: 13

Using Wav File: cello.wav

Splitting Stage

Key1 (Crypto Key): man2017 Length: 7

HMAC-SHA256 Value: 235fb6540d2a5fce62b012728e3b3d8136f9195fc41bbb73a5a86b1af7a2492a

Key2: EMAN@e Length: 6

Crypto Stage

Encrypted Key: EAAAAPYpgP1ZcyMIGke9RAuXdIbvEIZdbr0kbvq+FlzPiXuB

Stego Stage

● Linear ○ Random

Result:

```
Using linear steganography algorithm (Fastest)
Audio loaded Samples found: 2
Maximum file size for this file = 0.00 B - (file size digits + file name character count) bytes
Text encrypted 8foV67L29hU/fdzpQ3rHTWr7OOdl+q/Lg8gs71bo5YE=
```

Figure 2-Test Result

From result, the system checked the length of password (which is 13 for password used in test), then it split the password to Key1 (7 characters) and Key2 (6 characters), as described in 4. The Key1 used as crypto key for Key2, in same time the Key1 will pass to HMAC SHA256 to generate hash value that will send to server, then AES encrypted result for Key2 and encryption result by HMAC-SH265 for Key1 are shown in Figure- 2. The encrypted result of Key2 will then embed within the wave file by used LSB algorithm in either liner or random method. The process run in fast no any notable hung or error, also the wave file that used in imbedding method are relatively small.

6. Conclusion

Securing the user password by encryption and embedding it in audio file is providing high security. In this work a crpto-stego authentication model has been design that combined the advantage of the two techniques. The user password is separated into two parts one encrypted by used HMAC-SH256 hash algorithm and transfer to server, while the second is encrypted by AES-256 then used LSB algorithm to imbed the ciphertext within audio file then transfer to server. The method is successfully operated, and the authentication process has run smoothly in both login and registering without any problem. Because the model transfer password in two separated parts and used two different technique for encryption in addition to used stego to hided part of password, this makes the proposed method withstand different attacks and thus a very strong and secure method of password protection can be obtained.

7. Reference

1. Shinde M. P., Shelke P., Pawar P., Ranade K. and Prof. Shinde J. V. **2014**. *International Journal of Technical Research and Applications*. **2**(3): 84-86.

2. Koduri N. **2011**. Information Security Through Image Steganography Using Least Significant Bit Algorithm. Master of Science in Information Security and Computer Forensics, University of East London.

3. Sharma B. and Singh S. **2016**. A Review Paper on Different Network Security Techniques in Wireless Communication. *International Journal for Research in Technological Studies*, **3**(9): 8-10.

4. Kumar R. B. and Murti. P.R.K. **2014**. Data Security and Authentication Using Steganography. *International Journal of Computer Science and Information Technologies* (IJCSIT), 2(4): 1453-1456

5. Yang W. C. and Wen C. Y. **2008**. *Applying public key water marking techniques in forensic imaging to preserve the authenticity of the evidence*. 2008Workshop, LNCE 5075, Springer verlag Berlin Heidelberg, pp278-287.

6. Asad M., Gilani J. and Khalid A. **2011**. An Enhanced Least Signifcant Bit Modifcation Technique for Audio Steganography. 2011 international conference on Computer Networks and Information Technology (ICCNIT), pp.143-147.

7. Djebbar F., Ayad B. and Habib Abed-Meraim H. K. **2011**. A view on latest audio steganography techniques. 2011 International Conference on Innovations in Information Technology, pp.409-411.

8. Sathya V., Balasubramaniyam K. and Murali N. **2012**. Data hiding in audio signal, video signal text and JPEG Images. IEEE-International Conference on Advances in Engineering, Science and Management (IEEICAESM 2012), pp74l -746.

9. Guizani S. and Nasser N. **2012**. An Audio/ Video Crypto Adaptive Optical Steganography Technique. IEEE 2012, pp, 1057-1062.

10. Pathak P., Chattopadhyay A. K. and Nag. A. **2014**. A New Audio Steganography Scheme based on Location Selection with Enhanced Security. 2014 First International Conference on Automation, Control, Energy and Systems (ACES). pp.1-4.

11. Kumar P. P., Bhagat R. and Suvarna S. **2017**. *Steganography Using Visual Cryptography*. Book, Independently Published, Pratheek, ISBN-13: 978-1520478364.

12. Ayushi. **2010**. A Symmetric Key Cryptographic Algorithm. *International Journal of Computer Applications*, **1**(15): 1-4.

13. Nitasha and Sood N. **2014**. Review on: Enhancing the Security of Multilevel Audio Steganography Using AES. *International Journal of Advanced Research in Computer Science & Technology* (IJARCST), **2**(2): 270-273.

14. Indrayani R., Nugroho H. A., Hidayat R. and Pratama I. **2016**. Increasing the Security of MP3 Steganography Using AES Encryption and MD5 Hash Function. International Conference on Science and Technology-Computer (ICST), IEEE, 2016.