Volume 4, Issue 5, May 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Comparative study of Hashing Algorithm Using Cryptographic and Steganography Using Audio Files

Sangeeta Raheja
Pursuing M.Tech
Manav Rachna International University, Faridabad
India

Shradha Verma
Assistant Professor
Manav Rachna International University, Faridabad
India

Abstract-:- In these days sharing the information over the internet becoming a critical issue. So numbers of techniques are available to protect the data. The present work will focus on the combination of hashing, cryptography and steganography to secure the data. Firstly from the original data the hash value is produced. For hash value SHA (Secure hash algorithm) is used. Secondly the data is encrypted by using cryptography algorithm like AES is used. Now the hash value and encrypted data must be hidden in image or video or audio file for securing the data. At the receiver end the hash value is matched and data is decrypted by using decryption technique.

Keywords—Cryptography, SHA-1, SH256, SHA512, LSB

1. Introduction

Today the use of internet for communication has increased. So the security of information is important issue for safety. Cryptography is a technique of securing the information. The Cryptography is used for encrypting and decrypting the data. Encryption means convert the plain text into cipher text. The decryption means convert the cipher text into plain text. The encryption is done at the sender side and decryption is done at the receiver side. Cryptography is classified into symmetric cryptography and asymmetric cryptography. The symmetric key means same key is used for encryption and decryption at the sender and receiver end. The asymmetric key means different key is used for encryption and decryption at the sender and receiver end. Hashing is a function of cryptography that produces the hash value. The hash value is an arbitrary-length string that provides the integrity as well as authentication. The hash value is a one way function.

A. Terms Used In Cryptography

Plain text: - The original message that the person want to send is called plain text. For an example Neeraj is a person wishes to send "how are you" message to Meeta. The message "how are you" is a plain text.

Cipher text: - The message that cannot be understood by anyone is called cipher text. The cipher text is produced from plain text. The "%adgh=$dgfh" is a cipher text of message "how are you".

Encryption: - when plain text is converted into cipher text then the cipher text is called encryption. For encryption the algorithm like AES or DES is used.

Decryption: - When cipher text is converted into plain text then it is referred as decryption. It also need two things decryption algorithm and key. Key:-When numeric or alpha numeric text or special symbol is combined then it is referred as key. Key plays a very important role in cryptography.

2. Literature Review

In this section the various performance factors and technique for hashing , encrypting and hiding the data used by various papers are listed. In the research paper [1] proposed that the cost of implementing a SHA-512 algorithm gives a 50 percent performance improvement over SHA-256. In the research paper [2] proposed Audio steganography with encrypted data that increases the security. In the proposed system the key management is also used in both sender and receiver to make the system more secure. In research paper [3] concluded that AES is a cryptographic algorithm that is used for encryption and decryption. The AES is more secure and faster than Triple DES algorithm. The paper also proposed about the sha-1 algorithm where the key is hashed using hash algorithm.
In research paper [4]proposed about AES,DES and RSA algorithm with LSB substitution technique. In the proposed system the performance of these algorithm are analyze. Based on these analysing it was concluded that AES consumes least encryption and decryption time as compare to DES and RSA. But RSA algorithm has more encryption time.

3. Proposed Work

In these days securing the data is very big issue for the computer users. In this proposed system we implement and compare the three hashing algorithms for producing the hash value and then the original data is encrypted by using cryptographic algorithm. The data is encrypted by using AES algorithm. Now the hash value and cipher text will be

hidden behind audio file by using LSB substitution technique. In the proposed system we are doing this to improve the security that is very big issue in these days.

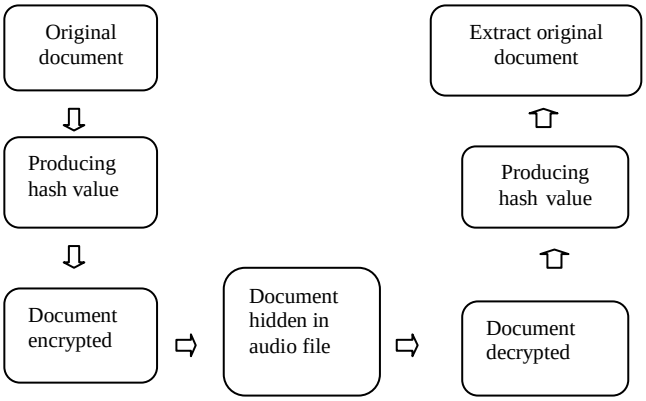

Figure-1: Proposed work

In the proposed system three techniques used as shown in fig. First to produce the hash value we compare and analyze three different hashing algorithms. Secondly data is encrypted by using cryptography algorithm. Thirdly the hash value and encrypted data is hidden within audio file. At the receiver end the document is extracted from audio file. Then the document is decrypted. From this document the hash value is produced . The hash value is matched and the original document is extracted.

4. Hashing Algorithms

A. SHA-1(Secure Hash Algorithm)

Secure Hash algorithm1. It is a hashing function used to produce the hashing value. It produces the hash value of 160 bits (20bytes). It has the 80 number of rounds. The user which has the hash value can modify the data. The hashing algorithm provides authenticity and integrity. If any user modifies the data then the hash value will be changed.

B. SHA-256(Secure Hash Algorithm)

It is a hash function used to produce the hash value. It belongs to SHA-2 family. It produces the hash value of 256 bits(32 bytes). It has number of 80 numbers of rounds. It is the improvement version of SHA-1. It is more secure and faster than SHA-1 algorithm.

C. SHA-512(Secure Hash Algorithm)

It is a hash function used to produce the hash value. It also belongs to SHA-2 family. It produces the value of 512bits (64 bytes). It has total 64 numbers of rounds. It is faster and secure than SHA-256 algorithm.

D. Factors Analyzed

Table 1: Analysis of various factors

S.NO	Factor Analyzed	Sha-1	Sha-256	Sha-512
1	Message digest size	160	256	512
2	Block Size	512	512	1024
3	Rounds	80	80	64
4	Collision found	Yes	No	No
5	Word size	32	32	64

5. Encryption algorithm

In cryptography the data is converted from plain text to cipher text. The cipher text is the text that cannot be understand by any other person. When the plain text is converted into cipher text then it is called encryption. When the cipher text is converted into plain text then it is called decryption. For encryption the AES algorithm is used. The full form of AES is Advance Encryption Standard. The AES provides security as well great speed. The AES replaces the DES algorithm. The AES can be used on various platforms. In AES algorithm 10,12 and 14 rounds. The AES uses key size of 128,192, or 256 bits. AES is very strong cryptography algorithm because of security , cost and implementation. AES is very strong algorithm that it has proved against many attacks such as brute-force attack. AES can be implemented on the cheap processors and a minimum amount memory.

In AES each round of the encryption process requires a series of steps .these steps consists of four operations.

a. Sub Bytes :This is very simple operation that converts every bite into different value.
b. ShiftRows : in this operation every row is rotated to the right by a certain number of bytes.
c. MixColumns :In this operation every coloumn of the state array is processed separately to produce a new coloumn. The old one is replaced by new coloumn.
d. XorRoundKey : This is the operation that takes only existing state array.

6. Data Hiding

In cryptography data is hided by using steganography. It is method of hiding information. The data can be hided behind audio, video and image. For steganography the LSB substitution technique is used. The steganography is a technique of hiding the data in this way only the sender and receiver can view the message. The data can be hided behind:

I. Audio steganography
II. Video steganography
III. Image steganography

I) Image steganography :Least Significant Technique is used of image steganography. If the leats bit is changed then that causes the little change to the original value. If the image is 24-bit , there are 3bytes of data to represent RGB values for every pixel. It means the 3 bits can be stored in every pixel.

II) Audio steganography: In the audio steganography the data will be hided behind audio file to hide the data behind audio is something similar to image steganography. In audio steganography the data is hided behind samples. For samples the sampling technique is followed. Sampling technique converts analog audio signal to digital binary sequence.

III) video steganography: To hide the data behind vedio file the LSB modification algorithm is used. In this watermark channel bit rate is very high and a low computational complexity. In this 3 bits are stored per pixel.

7. Experimental Results

The experimental results of hashing algorithms are implemented in Visual studio Net packages. The above said hashing algorithms are compared on the basis of time. In this paper we are comparing three algorithms like SHA-1, SHA-256 AND SHA-512. The SHA-512 is giving the better result.

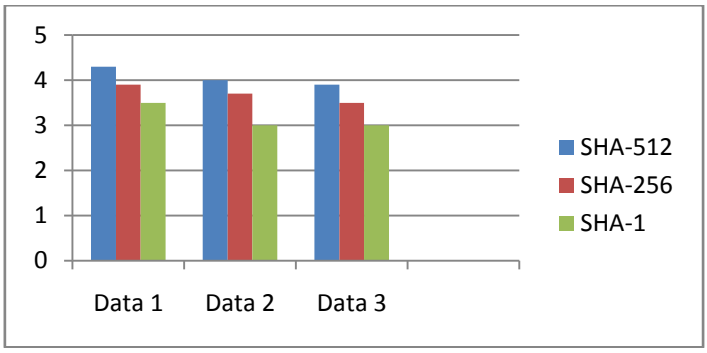

Figure 2.Comparative status of time among Sha-1,Sha-256,Sha-512.

8. Conclusion:-

In Data communication, cryptography has their own importance. Our research work surveyed the existing hashing techniques like SHA-1, SHA-256 and SHA-512 algorithms along with encryption and LSB substitution technique. Those hashing techniques are analyzed. Based on the experimental result it was concluded that SHA-512 algorithm consumes least time for producing hash value as compared to SHA-256. But SHA-1 consumes more time for producing hash value.

References

[1] Yaser Esmaeili Salehani1, S. Amir Hossein A.E. Tabatabaei,Mohammad Reza Sohizadeh Abyaneh3, Mehdi Mohammad Hassanzadeh "NESHA-256, NEw 256-bit Secure Hash Algorithm" Sharif University of Technology, Tehran.
[2] Shay Gueron , Simon Johnson , Jesse Walker " SHA-512/256" Security Research Lab, Intel Labs, Intel Corporation, USA.
[3] Masoud Nosrati Ronak Karimi Mehdi Harir "Audio Steganography: A Survey on Recent Approaches" World Applied Programming, Vol (2), No (3), March 2012. 202-205.
[4] Ritu Pahal Vikas kumar " Efficient Implementation of AES" SGI Samalkha, Haryana, India Volume 3, Issue 7, July 2013.
[5] Tanmaiy G. Verma1, Zohaib Hasan2, Dr. Girish Verma3 " A Unique Approach for Data Hiding Using Audio Steganography" International Journal of Modern Engineering Research (IJMER) www.ijmer.com Vol. 3, Issue. 4, Jul - Aug. 2013 pp-2098-2101.

[6] Debnath Bhattacharyya, Poulami Das, Samir Kumar Bandyopadhyay and Tai-hoon Kim, Text Steganography: A Novel Approach, Research paper , International Journal of Advanced Science and Technology, Vol. 3, February, 2009 .
[7] Arvind Kumar, Km. Pooja, Steganography- A Data Hiding Technique, Research paper , International Journal of Computer Applications (0975 – 8887) Volume 9– No.7, November 2010.
[8] Masoud Nosrati, Ronak Karimi, Mehdi Hariri, An introduction to steganography methods, World Applied Programming, Vol (1), No (3),August 2011. 191-195.
[9] Bender W, Gruhl D & Morimoto N (1996) Techniques for data hiding. IBM Systems Journal 35(3): p 313–336.
[10] Nedeljko Cvej, Algorithms for audio watermarking and steganography, Oulu 2004, ISBN: 9514273842.
[11] Sos S. Agaian, David Akopian, Sunil A. D'Souza1, Two algorithms in digital audio steganography using quantized frequency domainembedding and reversible integer transforms, USA.
[12] M. Matsui, "Linear Cryptanalysis Method for DES Cipher",EUROCRYPT, LNCS 765, pp.386-397, Springer, 1994.
[13] I. Ben-Aroya, E. Biham, "Differential Cryptanalysis of Lucifer", CRYPTO,Journal of Cryptology, pp.187-199, Springer, 1994.
[14] D. Wagner, "The Boomerang Attack, Fast Software Encryption", 6thInternational Workshop on Fast Software Encryption, LNCS 1636, Springer,1999.
[15] A. Biryukov, "The Boomerang Attack on 5 and 6-Round Reduced AES",LNCS 3373, pp.11-15, Springer, 2005.
[16] L. Knudsen, "Truncated and Higher Order Differentials", 2nd International Workshop on Fast Software Encryption, LNCS 1008, pp.196–211, Springer,1994.
[17] J. Daemen, L. Knudsen, V. Rijmen, "The Block Cipher Square", 4th International Workshop on Fast Software Encryption, LNCS 1267, pp. 149–165, Springer, 1997.
[18] T. Jakobsen, L. Knudsen "The Interpolation Attack on Block Ciphers", 4thInternational Workshop on Fast Software Encryption, LNCS 1267, pp.28–40,Springer, 1997.
[19] J. Daemen, V. Rijmen, "AES Proposal: Rijndael, Version2", http://www.esat.kuleuven .ac.be/vijmen/rijndael , 1999.
[20] Kazumaro Aoki and Yu Sasaki. Preimage attacks on one-block MD4, 63-step MD5 and more. In SelectedAreas in Cryptography'08, volume 5381 of Lecture Notes in Computer Science, pages 103–119. Springer,2008.
[21] Ishaque, M. Qudus Khan, F. Abdul Sattar, S. Investigation of SteganalysisAlgorithms for Multiple Cover Media. Ubiquitous Computing andCommunication Journal. Vol 6, no 5, October 2011.

