Implementation of Secure Hash Algorithm-1 using FPGA

Vishakha P. Borkar[1], Mrs. A. S. Khobragade[2]

[1]M. tech. Student
Department of Electronics Engineering
Priyadarshini College of Engineering, Nagpur.
Borkarvishakha17@gmail.com

[2] Professor
Department of Electronics Engineering
Priyadarshini College of Engineering, Nagpur

Abstract-:- ***Sharing of information over the internet becoming a critical issue. To secure the data lotsof techniques are available. The present work will focus on the combination of hashing, cryptography and stenography to secure the data. Hash value will obtained from original data. Secure hash algorithm is use for hash value. Then the data is encrypted by using cryptography algorithm. Now the hash value and encrypted data must be hidden in image or audio or video file to secure the data. At the receiver end the hash value is match and data is decrypted by using decryption technique.***

Keywords— FPGA, hash function, Secure Hash Algorithm-1 (SHA-1), Verilog HDL.

1. INTRODUCTION

Today the use of internet for communication has greater than before. So the security of information is significant issue for safety. Cryptography is a method of securing the information. For encrypting and decrypting the information, cryptography is useful. Encryption means convert the simple text into cipher text. The decryption means translate the cipher text into plain text. The encryption is completed at the sender side and decryption is completed at the receiver side. Cryptography is divided into asymmetric cryptography and symmetric cryptography. The symmetric key means same key is use at sender and receiver for encryption and decryption. The asymmetric key means different key is use for at sender and receiver for encryption and decryption. Hashing is a role of cryptography that produce the hash value. The hash value is an arbitrary-length cord that provides the reliability as well as confirmation. The hash value is a one way function. Hash functions play a major role in today's cryptographic applications. SHA (Secure Hash Algorithm) is a legendary message compress standard use in computer cryptography, it can condense a long message into a short message. The SHA-1 Verilog source code is separated into three modules, namely Initial, Top and Round module. The Verilog code is assemble on Virtex5 FPGA using Xilinx ISE software tool. A comparison between desire SHA-1 hash function implementation in the company of supplementary works shows that it achieves a high output and clock frequency.

1.1. SHA-1Hashing Algorithm

The hashing function i.e. Secure Hash algorithm-1 is use to produce the hashing value. It produces the hash value of 160 bits that is 20 bytes. It has the 80 number of round. The user which has the hash value can modify the data. The hashing algorithm provides accuracy and reliability. If any user modifies the data then the hash value will be changed. SHA-1 is a complex algorithm that include multiple 32-bit, 5-way additions, complex logical functions, data shifting and a great contract of return. Commonly implementations of the SHA -1 algorithm have required large die areas and so made moderately expensive portable device. A propose method has been applied to be relatively inexpensive one. The architecture is offered for SHA -1 hash function. The implementation is carried out by Verilog HDL on Xilinx FPGA device. The synthesis grades are compare and present with other SHA -1 implementations.

Here, the hardware terms of system performance, operating frequency and covered area are compared. The hash algorithms, also called as message digest algorithms which generating a single fixed length bit vector for an arbitrary-length message. The bit vector is called the hash of the message and it is noted as H. This hash value should be the same each time the same input is hashed. A hash function utilize in cryptography is one way and collision resistant. The purpose of a hash function is to generate a fingerprint of a file, message or may be other block of data. Hash function must have the following requirements:

II.1. Weak collision resistance: For any given block x, it is computationally infeasible to find y with H(x) = H(y).
II.2. Strong collision resistance:- For several given block x, it is computationally infeasible to find x, y with H(x) = H(y).
II.3.One-way property:- For any given value h, it is computationally infeasible to find x with H(x) = h.

SHA (Secure Hash Algorithm) is intended by National Security Agency of the U.S.A. It is a message compress standard use to co-operate DSS (Digital Signature Standard) Technology. Alhough SHA is design for DSS, it will be useful in lots of protocols and secure algorithm. The basic version of SHA is called SHA or SHA -0. SHA-1 is the better version of SHA -0.

1.2 Data Hiding

In cryptography data is hide by means of steganography. It is

process of hiding information. The data can be hided beside image, video and audio. For steganography, LSB replacement technique is use. The steganography is way to hide data in this that only sender and receiver can view the message. The data can be hide behind:

III.1. Image steganography
III.2. Audio steganography
III.3. Video steganography

Image steganography :Least Significant Technique is use for image steganography. If the LSB is changed then that cause the small change to the original value. If the image is of 24 -bit , there is 3 byte of data to present RGB values for every pixel which shows that the 3 bits can be stored in every pixel.

Audio steganography: In case of audio steganography, the data will be hide at the back of audio file to hide the data behind audio is somewhat matches to image steganography. In audio steganography the data is hided behind samples. For samples, the sampling technique is follow. Sampling technique converts analog audio signal to digital binary sequence.

Video steganography: In this case the data is hide behind the video file the LSB modification algorithm is used. In this watermark channel bit rate is much high and it has low computational complexity. In this 3 bits are store per pixel.

1.3SYNTHESIS AND DESIGN OF SHA-1

The input message of SHA-1 is no longer than 264bits can generate a 160 bit message abstract. The input is process in 512-bit blocks. The algorithm processing involve the following steps:

IV.1.**Padding:** The aim of message padding is to make the total length of a padded message matching to 448 module 512. The number of padding bits is among 1 and 512. Padding consists of 1 single bit which follow a series of 0-bit.

IV.2.**Appending Length:** A 64-bit binary account of the original length of the message is appended to the end of the message.

IV.3.**Initialize SHA- Buffer:** The message digest is computed with the help of last padded message. The computation uses two buffers, in which each one consist of five 32-bit words and a sequence of eighty 32-bit words.

IV.4. **Hash Calculation**

IV.5**. Output**

2. Literature Survey

As time passes a lot of improvement and work is done on secure hash algorithm for data security purpose .The basis idea of secure hash algorithm-1 is to improve security of information during data communication. The secure hash algorithm is a function of cryptography that generates the hash value that provides the integrity as well as authentication.
The paper [1] resulted that SHA-1 architecture achieves a higher working frequency and also higher throughput.
The paper [2] represent functionality of hash algorithm for the purpose of security.
The paper [3] describes the utility of hash algorithm in various applications.

3. Proposed Plan

In the recent days, security of data is very essential issue for the computer users. In this proposed system we implement and hashing algorithms for producing the hash value. The original data is encrypted by using cryptographic algorithm. The data is encrypted by using hash-1 algorithm. The hash value is hide behind audio file by using LSB substitution technique. The proposed system definitely plays an important role to improve the security which is great issue in these days.

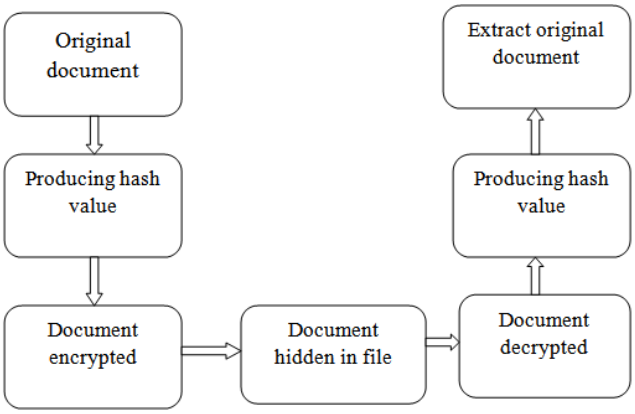

Figure.1 Proposed work

Proposed system contain three techniques as shown in fig. First to produce the hash value and then compare, analyze three different hashing algorithms. After it the data is encrypted by using cryptography algorithm. At last the hash value and encrypted data is hidden inside audio file. At the receiver end the document is extract from audio file. Finally the document is decrypted. From this document the hash value is produced. The hash value is coordinated and the original document is extract.

4. Conclusion

In data communication, cryptography has their own importance. Our research work surveys the existing hashing techniques like SHA-1algorithms along with encryption and LSB substitution technique. The propose SHA-1 architecture has capability to achieves a higher working frequency and also higher throughput. Hash algorithm is use as components by other cryptographic algorithms and process to provide information security services.

5. References

[1].International Journal of Information and Computation Technology. ISSN 0974-2239 Volume3, Number 8 (2013), pp. 757-764 © International Research Publications House .
[2].International Journal of Emerging Technology and Advanced Engineering. ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 2, Issue 12, December 2012.

[3].Quynh Dang, "Recommendation for Applications Using Approved Hash Algorithm", NIST special publication 800-107, Computer security Division National Institute of Standards and Technology, Dept of commerce, USA, pp. 1-21, 2011.

[4].Cheng Xiao-hui and Deng Jian-zhi, "Design of SHA-1 Algorithm based on FPGA", IEEE Second International Conference on Networks Security,Wireless Communications and Trusted Computing, (NSWCTC), Vol-1, pp.532-534, 2010.

[5] Zhou Hua and Liu Qiao, "Har dware Design for SHA-1 Base d on FPGA",IEEE International Conference Publications on Electronics, Communications and Control (ICECC), pp.2076-2078, 2011.

[6] Cheng Xiao-hui and Deng Jian-zhi, "Design of SHA-1 Algorithm b ase d on FPGA", IEEE Second International Conference on Netw orks Security , Wireless Communications and T rusted Computing, (NSWCTC), V ol-1, pp.532-534, 2010.

[7]. A.G.Konheim and Ebooks Corporation., Computer Security and Cryptography. Hoboken:John Wiley & Sons Inc., 2007.

[8].William Stallings, "Cryptography and Network Security, Principles and Practices" Fourth Edition , 2005 .