

# Implementation of Secure Hash Algorithm-1 using FPGA

Vishakha P. Borkar<sup>1</sup>, Mrs. A. S. Khobragade<sup>2</sup>

<sup>1</sup>M. tech. Student  
Department of Electronics Engineering  
Priyadarshini College of Engineering, Nagpur.  
Borkarvishakha17@gmail.com

<sup>2</sup> 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 lot of techniques are available. The present work will focus on the combination of hashing, cryptography and steganography to secure the data. Hash value will be obtained from original data. Secure hash algorithm is used 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 matched 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 used at sender and receiver for encryption and decryption. The asymmetric key means different key is used for at sender and receiver for encryption and decryption. Hashing is a role of cryptography that produces the hash value. The hash value is an arbitrary-length code 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 compression standard used 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 assembled on Virtex5 FPGA using Xilinx ISE software tool. A comparison between desired SHA-1 hash function implementation in the company of supplementary works shows that it achieves a high output and clock frequency.

### 1.1. SHA-1 Hashing Algorithm

The hashing function i.e. Secure Hash algorithm-1 is used to produce the hashing value. It produces the hash value of 160 bits that is 20 bytes. It has the 80 number of rounds. 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 includes multiple 32-bit, 5-way additions, complex logical functions, data

shifting and a great amount of return. Commonly implementations of the SHA-1 algorithm have required large die areas and so made moderately expensive portable devices. A proposed 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 compared and presented 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 generate 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 used in cryptography is one-way and collision resistant. The purpose of a hash function is to generate a fingerprint of a file, message or any 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 compression standard used to co-operate DSS (Digital Signature Standard) Technology. Although SHA is designed for DSS, it will be useful in lots of protocols and secure algorithms. 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 hidden by means of steganography. It is

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

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

**Image steganography**: Least Significant Technique is used for image steganography. If the LSB is changed then that causes the small change to the original value. If the image is of 24-bit, there is 3 bytes 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 hidden at the back of an audio file to hide the data behind audio. It somewhat matches to image steganography. In audio steganography, the data is hidden behind samples. For samples, the sampling technique is followed. Sampling technique converts an analog audio signal to a digital binary sequence.

**Video steganography**: In this case, the data is hidden behind the video file. The LSB modification algorithm is used. In this watermark channel bit rate is much higher and it has a low computational complexity. In this, 3 bits are stored per pixel.

### 1.3 SYNTHESIS AND DESIGN OF SHA-1

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

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

**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 the last padded message. The computation uses two buffers, in which each one consists 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 algorithms for data security purposes. The basic idea of a secure hash algorithm-1 is to improve the 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.

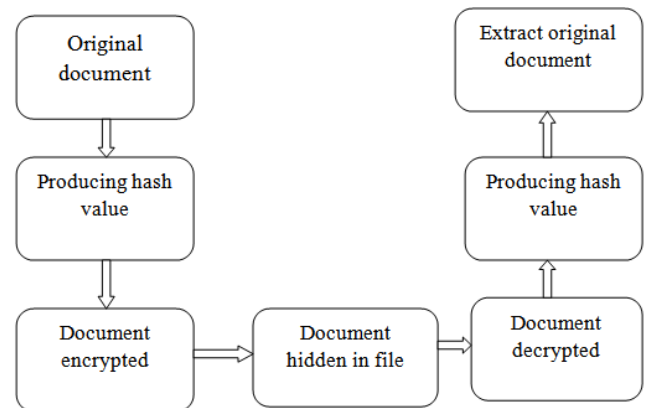
The paper [1] resulted that SHA-1 architecture achieves a higher working frequency and also higher throughput.

The paper [2] represents the functionality of a hash algorithm for the purpose of security.

The paper [3] describes the utility of a hash algorithm in various applications.

## 3. Proposed Plan

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



**Figure.1** Proposed work

The proposed system contains three techniques as shown in the figure. First, to produce the hash value and then compare, analyze three different hashing algorithms. After that, the data is encrypted by using a cryptography algorithm. At last, the hash value and encrypted data are hidden inside an audio file. At the receiver end, the document is extracted from the 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 extracted.

## 4. Conclusion

In data communication, cryptography has its own importance. Our research work surveys the existing hashing techniques like SHA-1 algorithms along with encryption and LSB substitution techniques. The proposed SHA-1 architecture has the capability to achieve a higher working frequency and also higher throughput. Hash algorithms are used as components by other cryptographic algorithms and processes to provide information security services.

## 5. References

- [1]. International Journal of Information and Computation Technology. ISSN 0974-2239 Volume 3, 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, “Hardware Design for SHA-1 Based 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 based on FPGA”, IEEE Second International Conference on Networks Security, Wireless Communications and Trusted Computing, (NSWCTC), Vol-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 .

