Information Authentication Testing using Message Digest Algorithm

Ekta Brahmbhatt[1] H.G.Bhatt[2]
[1,2]Department of Computer Engineering
[1,2]Sankalchand Patel College of Engineering, Visnagar, India

Abstract— This paper proposes hash algorithms for the images A hash function is any function that can be used to map data of arbitrary size to data of fixed size. Hashes are used to secure the data and message integrity, password validity, and are the basis of many other cryptographic systems. Hashes are unique and it is one way function. It cannot be reversed. We use a SHA-512 algorithm and also try to reduce the brute force attack with the help of 2D logistic map method.SHA-512 is the most secure algorithm. Chaotic system has high sensitivities to its initial values, high sensitivities to its parameter(s), the mixing property and the ergodicity. Simulation results are shown.

Key words: 2D Logistic Map, SHA-512, Chaotic Map

I. INTRODUCTION

In this era of technology electronics and communication has become an integral and most important part of everyone's life. Because it is simpler, fast and more secure with adoption of electronics and communication on such a large scale it has become necessary to transmit the data more securely. Cryptographic hash functions remain one of the most important cryptographic primitives, and they can be used to guarantee the security of many cryptographic applications and protocols such as digital signature, random number generation, data source authentication, key update and derivation, message authentication code, integrity protection, malicious code recognition, SSL, TLS and S/MIME.

In cryptography plain text image or data will be encrypted and decrypted with the help of secret key whereas in hash function we can't decrypt the data and can't get back the original data from the hash. So, cryptography is reversible process and hash function is irreversible process.

Hash functions are classified in two classes. 1) unkeyed hash function known as Manipulation Detection Code. 2) keyed hash function are used to construct the MAC(Message Authentication Code). The MAC is widely used to provide data integrity and data origin authentication. The choice between a MAC and an MDC is application dependent. They are also classified as, namely hash functions based on block cipher, hash functions based on modular algorithm and dedicated hash functions.

Cryptographic hash function has four main properties. 1) It is impossible to generate the a message from its hash value except by trying all possible messages. 2) A small change to a message should change the hash value so extensively that the new hash value appears uncorrelated with the old hash value. 3)It is impossible to find two different messages with same hash value. 4) It is quick to calculate hash for any given message. Hash is a one way function.

There are different algorithms used for creating the hash like MD2, MD5, SHA-1, SHA-2 etc…but SHA-2 family consist of different 6 hash functions: SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256. SHA-512 computed with 64 bit word. Its length is 512 bit. SHA-512 is designed by National Security Agency (NSA). In MD5 algorithm possibility of collision found in less than 64 round, in SHA-0 possibility of collision found in less than 80 round whereas in SHA-512 collision 100% found in 80 rounds so, complexity is higher than the other algorithms. Output size of SHA-512 is 512, block size is 1024 and we can transmit 2^{128}-1 bits in one round.

The objective of this paper is to increase the security level of transmitting the data and we take the image as a data input. We also used the 2D logistic map method to increase the security. With the help of both SHA-512 and chaotic map method we used hash as a 256 bit key and generate the encrypted image. Key will not be randomly generated. We scrambling the generated hash and choose the 256 bit from the 512 bit key. Thus, higher security will be obtained.

II. BACKGROUND

A. SHA-512 Algorithm

The design steps of the hash function as shown below. Sender send the messge processed by MAC algorithm and secret key. Receiver check the message and its hash if both hash are same then the message is authenticate. And if the both hash are different then we authenticate that the something will be wrong and message will be changed.

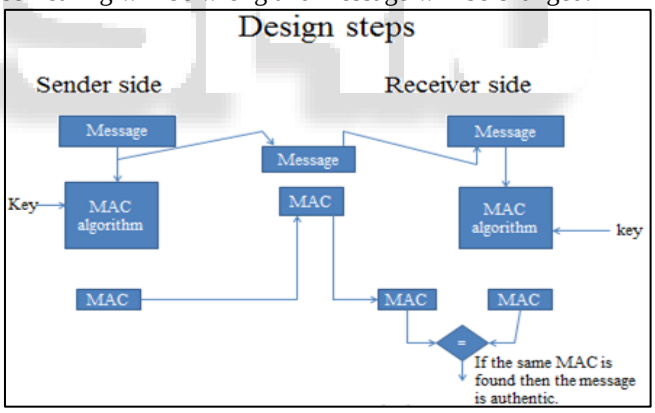

Fig. 1: Design steps of the hash function

B. SHA-512 Circuit Diagram

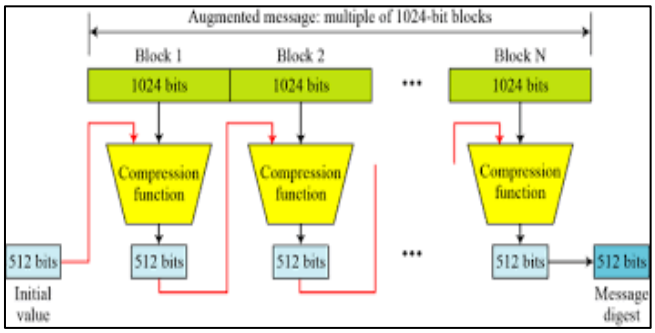

Fig. 2: Circuit Diagram of SHA-512

1) Steps of the algorithm SHA-512:

a) Step 1: Take the original hex message

Example: HELLO

b) Step 2: Convert hex message to decimal
Example: 65 32 101 115 116
c) Step 3: Convert decimal to binary
All the numbers are converted into the 8 bit binary for example 01000001
00100000
d) Step 4: Display binary message
e) Step 5: Calculate howmany '0' bits are padded and Append '0's' to the end
010000010010000001010100011001010111001101110100-
100000000000000000000000000000000000000000000000-
000000000000000000000000000000000000000000000000-
000000000000000000000000000000000000000000000000-
000000000000000000000000000000000000000000000000-
000000000000000000000000000000000000000000000000-
000000000000000000000000000000000000000000000000-
000000000000000000000000000000000000000000000000-
000000000000000000000000000000000000000000000000-
0000000000000000
f) Step 6: Append original message length
Original message was 48 characters long. So now add 58 zeros to the beginning of that number prior to adding it to the current message.
g) Step 7: Display pre-processed message and length of the Pre-processed message.
Example:
010000010010000001010100011001010111001101110100-
100000000000000000000000000000000000000000000000-
000000000000000000000000000000000000000000000000-
000000000000000000000000000000000000000000000000-
000000000000000000000000000000000000000000000000-
000000000000000000000000000000000000000000000000-
000000000000000000000000000000000000000000000000-
000000000000000000000000000000000000000000000000-
000000000000000000000000000000000000000000000000-
000000000000000000000000000000000000000000000000-
00000000000000000000000000110000
Message length was 512.
h) Step 8: 'Chunk' the message.
Convert it into 512*2 bits blocks.
i) Step 9: Break each chunk up into sixteen 32-bit words.
j) Step 10: 'Extend' into 80 words
Selecting four of the current words: [i-2], [i-15], [i-7] and [i-16] (here i = no. Of word created in step 9). 3 unique Left rotation (A,B,C) in the words w[i-2] and w[i-15]. Perform XOR

t = XOR(A[i-2], B[i-2])

Sigma1 = XOR(t , C[i-2]) (similarly for w[i-15] and create sigma2)
k) Step11: Combine (bit wise OR) sigma1, sigma2 and w[i-7] and w[i-16].
l) Step12: Initialize 8 constant variables and 4 diffrent functions, functions will be as following.

F1 = (B AND C) OR (!B AND D)
F2 = (B XOR C) XOR D
F3 = ((B AND C) OR (B AND D)) OR (C AND D)
F4 = same as function 2

Words will be divided into 4 groups and one function will be correspond to one group. Values obtain will combine with the constant words and obtained result will be message digest.

C. 2D Logistic Map (Chaotic Map):

In normal 2D logistic map method key will be random generated but in our case we take the hash as a key so more security we will obtain. We take the key of 256 bit but as we said that we use the SHA-512 so we will use 256 bit key from 512 bit. So complexity is higher than the normal 2D logistic map method.

In 2D logistic map method permutation, diffusion and transposition process will be occurred. Flow chart of proposed method is as shown below.

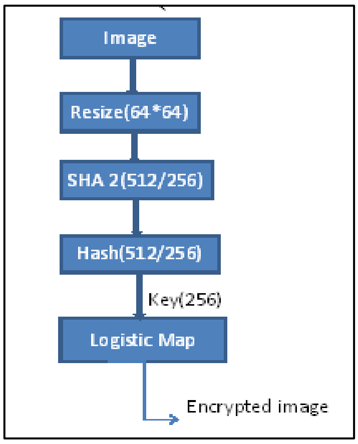

Fig. 3: Flow chart of proposed method

First we have to resize the image 64*64 bit RGB image. Then after apply the SHA-512 algorithm and generate the hash of this image. But hash is a length of 512 bit and we need only 256 bit key so after scrambling we take the 256 bit key from the generated hash which length is 512 bit and apply 2D logistic map method and we obtained the encrypted image.

1) Permutation Process:

In this process the pixels in plaintext image p have been well shuffled and the permuted image is unrecognizable. If the plain text image P is M×N then the total number of pixels in the image is MN. Sequence of x and y length of MN is generated with the help of 2D logistic map equation:

$$X_{i+}1=r(3y_i+1)x_i(1-x_i)$$
$$Y_{i+1}=r(3x_{i+1}+1)y_i(1-y_i)$$

Permutation matrix U^x and U^y can be obtained using the below equation:

$$U^x=[e^{r=1}{}_{\Pi x},\ e^{r=2}{}_{\Pi x},\ \ldots\ldots,\ e^{r=M}{}_{\Pi x}\ ]'$$
$$U^y=[e^{c=1}{}_{\Pi y},\ e^{c=2}{}_{\Pi y},\ \ldots\ldots,\ e^{c=N}{}_{\Pi y}\ ]'$$

2) Diffusion Process:

After sufficient number of cipher rounds any slight change in a plaintext image leads to significant changes in cipher text and thus attains the diffusion properties. After diffusion process plain text image becomes unintelligible. The least number of cipher rounds to have M×N changing pixels is

$$\#round_{min}=\log_{S\times S} M\times N=\log_2 MN/2\log_2 S$$

3) Transposition Process:

2D logistic transposition is achieved by shifting the each pixel in the plaintext image with the specified amount of the random integer image I over the integer space.

The ciphertext image of 2D logistic map C is defined as C = (P+I) mod F for the encryption, where F is the number of allowed intensity scales of the plaintext image. For example F=256 for a 8 bit gray scale image. For the decryption, P=(C-I) mod F.

III. RESULT AND DISCUSSION

Simulation results for message digest are shown below. In below given images, figure 4(a) is the digest of the original message. If we change the message then digest of the message will be changed. And this changed digest is shown in figure 4(b). We used 2D logistic map and this chaotic results are as shown in figure 4(c). In figure 4(c) original image and its encryption and decryption is shown. Histogram for original image and encrypted image is as shown in figure 4(d).

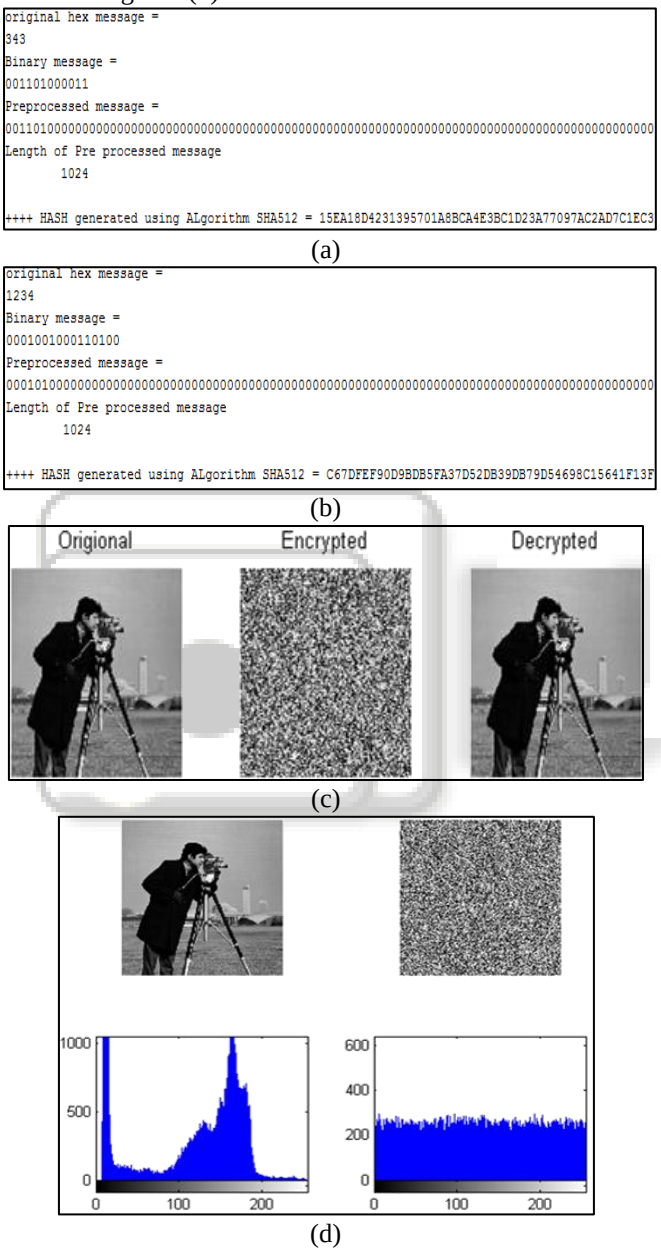

Fig. 4: Simulation results of message digest (a) digest of the message (b) changed message digest (c) chaotic results, (d) chaotic map results

IV. CONCLUSION

In this paper, we proposed a SHA-512 and 2D logistic map method for image and message authentication. We have applied secure hashing algorithm (SHA-2) for message digest and after applying this algorithm we have checked the authenticity of the message. We implemented Chaotic map encryption with random 256 bit key. This algorithm is proposed to reduce brute force attack. Various experimental results show that the proposed algorithm is more secure than the other algorithms.

ACKNOWLEDGMENT

I am beholden to express my obeisance to my mentor Prof. Hetal G. Bhatt for his hearty support and constant cultivation which is solemnly responsible in bringing our efforts to fruition.

REFERENCES

[1] Haider M. AI-Mashhadi, Hala B. Abdul-Wahab, Rehab F. Hassan, Computer Science Dept. University of Technology Baghdad, Iraq. "Secure and Time Efficient Hash-based Message Authentication Algorithm for Wireless Sensor Networks" 2014, IEEE

[2] Ren´e Romann, Ralf Salomon, University of Rostock Institute of Applied Microelectronics and Computer Engineering 18051 Rostock, Germany. "Salted Hashes for Message Authentication Proof of concept on Tiny Embedded Systems" 2014, IEEE

[3] Taqwa.A.Alhaj,Mariam.M.Taha,Faiza.M.Alim, "Synchronization Wireless Algorithm Based on Message Digest (SWAMD) For Mobile Device Database" International Conference On Computing, Electrical And Electronic Engineering (Icceee), 2013

[4] Saurabh Dey, Srinivas Sampalli, Faculty of Computer Science Dalhousie University, Canada, Qiang Ye Department of Computer Science University of PEl, Canada, "Message Digest as Authentication Entity for Mobile Cloud Computing" 2013,IEEE

[5] Zhiliang Zhu, Ke Zhai, Beilei Wang, Hongjuan Liu, Huiyan Jiang, Multimedia Medical Information Technology Laboratory, Software College, Northeastern University, Shenyang, China. "Research on Chaos-based Message Digest Method for Medical Images" 2009, IEEE

