International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 11 (2017) pp. 2707-2710

An Efficient Authentication Scheme using Extended Dynamic Chaotic map and Image Steganography

[1]B. Madhuravani and [2]Dr. P. Bhaskara Reddy

MLR Institute of Technology, Dundigal, Hyderabad, Telangana, India

[1]ORCID: 0000-0001-7412-1954, [2]ORCID: 0000-0003-2493-3633

Abstract:

There are many authentication protocols are used earlier, in the today's internet world we need more security for the online applications. Here we are using extended dynamic chaotic map, hop based image steganography, different cryptographic hash function, a dynamic cryptographic hash function, chaotic maps for the authentication, integrity, confidentiality. This model uses a novel parallel chaotic hashing model for single chaotic system to create an n-bit hash value for a given input data. Chaos based cryptographic algorithms are efficient approaches to create secure image encryption strategies as they have many important properties, for example the sensitivity dependence on starting conditions and system parameters, pseudorandom property, non-periodicity and topological transitivity. It provides high computational speed, bit variation, collision resistance, more security, less computation, limit memory resource as contrast to traditional parallel chaotic model. Steganography uses a hop variable and LSB steganography to embed the secret data into an object. Steganography hides the data from the unauthorized users using chaotic maps. This paper is introduced for providing authentication to the private data securely in the web.

Keywords: Steganography, Dynamic Cryptographic Hash Function, Hop variable, LSB Technique, Parallel Chaotic Map, Logistic Map, Mobile Computing, Integrity, Authentication.

INTRODUCTION:

Chaotic Maps are created to overcome the defects in the traditional Message Digest Hash Algorithms. The hash algorithms like SHA and MD5 developed cause less collision resistance were same key can produced for different files [1]. After MD5 [2], MD4 [3], SHA1 [4] and traditional methods are attacked there is an increase in effort to design a secure and efficient Hash function [5]. Traditional Chaotic functions are limited by their execution speed, particularly in mobile computing because of their limited resources. Parallel keyed functions are developed to overcome these defect, which in turn are susceptible to statistical attacks [6]. Complex Chaotic functions like Henon mapping and Rossler system are developed to solve the above mentioned issues[7]. In this paper we propose a parallel approach based multi chaotic system[8]. A chaotic maps in cryptography is used for the transmission of data safely and secretly without knowing to the third party[9]. If the third party involved in the transmission he cannot recognize the transmission. If we are using chaotic maps in cryptography they must be initially mapped to each other. If the chaotic parameters and also cryptographic keys can be mapped symmetrically to create satisfactory and functional outputs[10]. Chaotic theory is a arithmetic branch that deals with non linear dynamical systems. They are simple subtype of nonlinear dynamical systems. They contain very few interacting parts and these may follow very simple rules. These systems all have a very sensitive dependence on their initial conditions. Steganography is gaining importance recently due to the growth in secret communication between users over internet[11]. Steganography is the study of invisible communication which proposes different ways to hide a communicated message. In image stenography secret communication techniques are used to embed a message into cover image[12]. This cover image is used as a carrier to further embed the message and generate a stegoimage[13]. Stegoimage is the image which carries the hidden message. This strategies include digital signatures, covert channels, microdots, character arrangement, invisible inks, and spread spectrums communication[14].

PROPOSED TECHNIQUE:

In the proposed model a dynamic chaotic model is used to realize a more robust system of hash function which is both fast and secure than the traditional parallel chaotic maps. A dynamic cryptographic hash function and hop based steganography is used in this paper to achieve a secure method to transfer the message between two parties and also include authentication for the communication.

In this model the message digest is generated dynamically based on the input from user unlike the traditional methods where a fixed message digest is generated for an input.

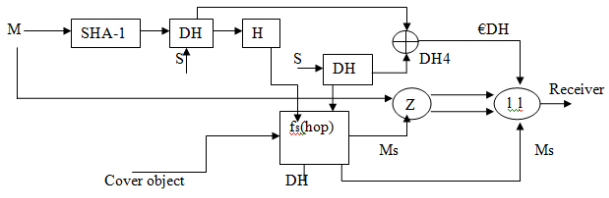


Figure 1: Encoding Algorithm.

The above figure 1 depicts the proposed method.

Where:

M = Original message
SHA-1 = Cryptographic hash function which generates hash code
DH = Dynamic cryptographic hash function which generates hash code
H = Hash code of M
S = MD Size
C = Cover Object
fs (hop) = Hop based Steganography encoding algorithm
Ms = Stego object
Hs = Hash code of Ms
€H = H XOR Hs

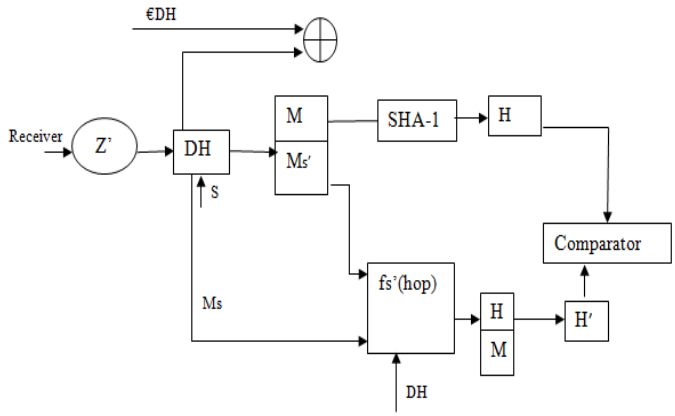


Figure 2: Decoding Algorithm.

The figure 2 above depicts the decoding procedure.

Algorithm: Encoding

1. During step1 the hidden data (M) is hashed by selecting SHA-1 hash function and generates message digest H.

2. The original text (M) and hash code (H) is embedded in to an image using dynamic hop image steganography technique and generates.

3. Ms and M together are send to receiver.

4. Hs and H XORed to get €H.

5. €H and Ms will be send as OTP to register mobile phone.

Algorithm: Decoding

1. At reception of OTP Ms is given inverse hop steganography model and retrieves H'.
2. Ms is given to inverse steganography algorithm to retrieve H' and M.
3. The retrieved H from inverse steganographic algorithm is compared with XORed €H and H.
4. Comparator function compares the calculated and received message digest.

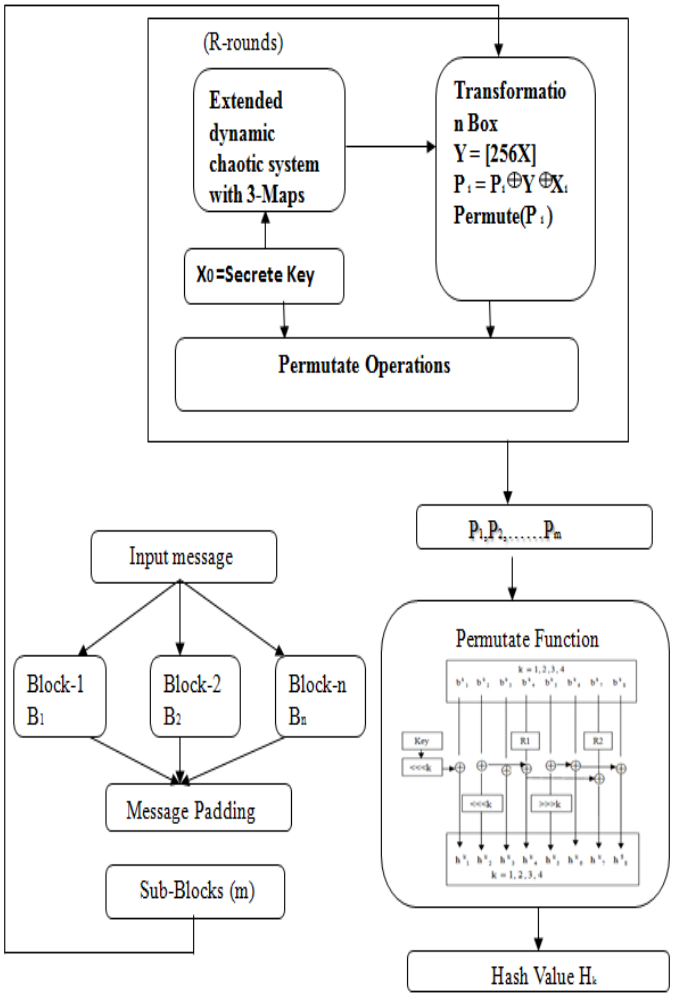


Figure 3: Extended Dynamic Permute Function Chaotic Model

EXPERIMENTAL RESULTS:

In order to exhibit the validity of algorithm, we present the experimental results. In this section, we perform various experiments to discover the productivity of our parallel hash function against traditional models. We also provide experimental results with traditional hash models in terms of hash sensitivity, confusion and diffusion. The proposed technique is simulated in java with plaintext and image documents. This has been tried for various images. The original image is shown in Fig 4(a) and 5(a) and the comparing steganography objects with different hash functions are shown in 4(b), 4(c), 4(d), 4(e), 4(f) and 5(b), 5(c), 5(d), 5(e), 5(f).

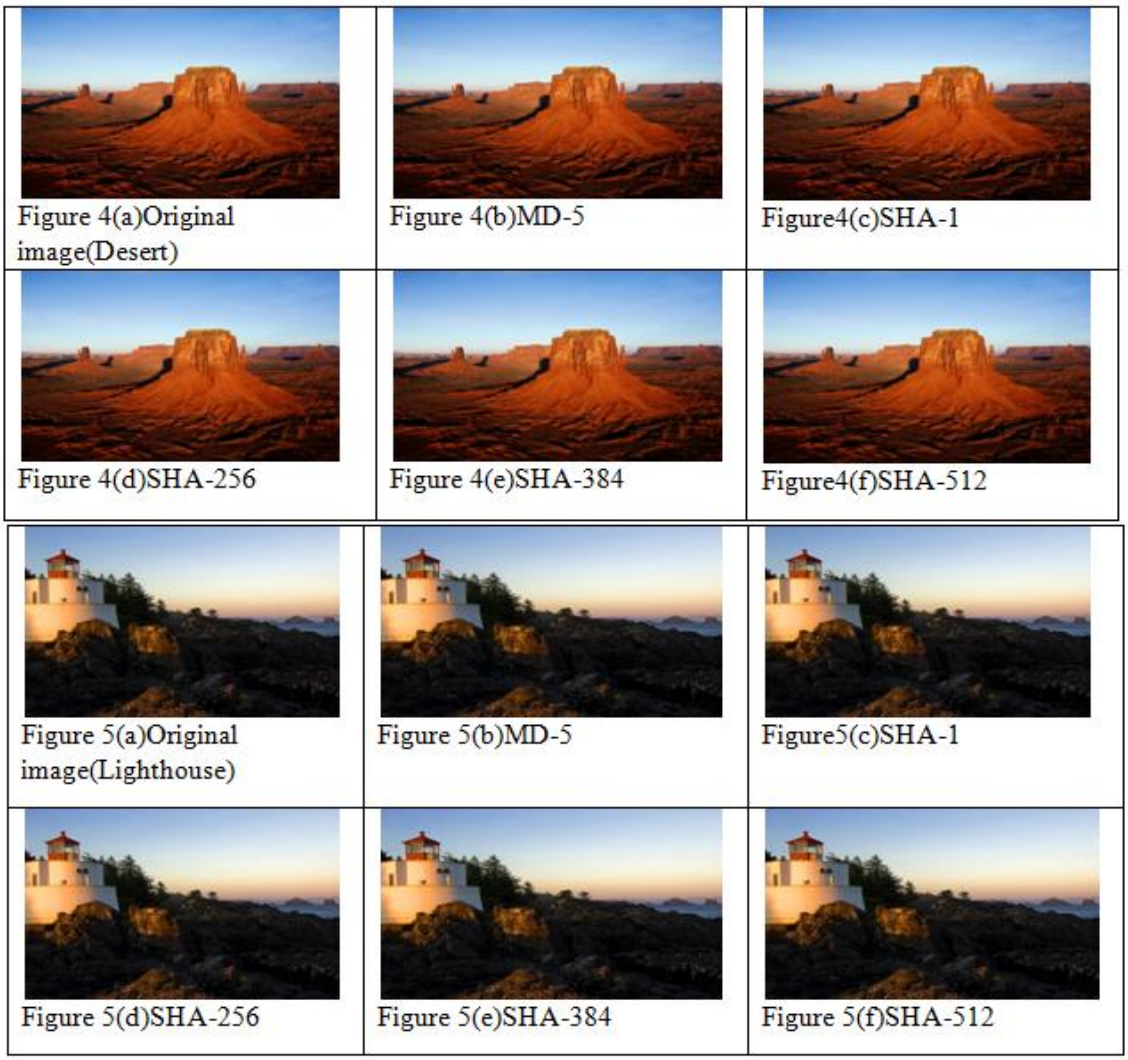


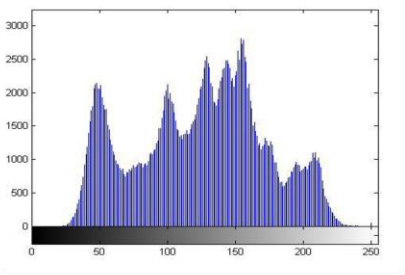
Figure 4(a)Original image(Desert) | Figure 4(b)MD-5 | Figure4(c)SHA-1

Figure 4(d)SHA-256 | Figure 4(e)SHA-384 | Figure4(f)SHA-512

Figure 5(a)Original image(Lighthouse) | Figure 5(b)MD-5 | Figure5(c)SHA-1

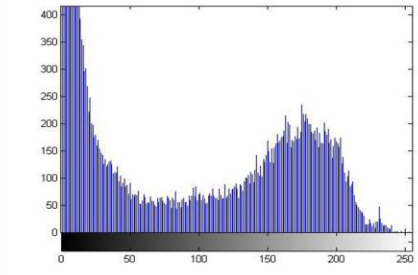
Figure 5(d)SHA-256 | Figure 5(e)SHA-384 | Figure 5(f)SHA-512

6(a)



6(b)

6(c)



6(d)

Figure 6 : 6(a)Cover Image, 6(b)Histogram Of Cover Image, 6(c)Stego Image, 6(d)Histogram of stego image

Stego Object Generation:

Table 1: Time to generate stego object.

Size	Text	Hop	Time to generate stego object(ns)							Size of stego object
			MD-5	SHA-1	SHA-256	SHA-384	SHA-512	LSB Steganography	Hop based Steganography	
Desert (1.64MB)	Hello	9	505257155	509127944	518516704	522749402	527761894	503256421	507127579	1.64 MB
LightHouse (1.92MB)	Hello world	6	507255127	511127673	523516622	529776610	535711604	505257492	506127609	1.92 MB

CONCLUSION:

In this paper, an efficient authentication scheme using extended dynamic chaotic map and image steganography is proposed. We propose a novel parallel chaotic hashing that assurance the randomness, high sensitivity and collision resistance of the structure and it is used to integrate multiple chaotic maps as a single chaotic system to generate an n-bit hash value for the given data. The proposed system is used for giving security to the online applications between two clients. This method is used for both audio and video steganography for hiding the data. Recreation comes about demonstrate that the calculation has a high capacity, a good invisibility, and that it is powerful for the normal image processing like JPEG compression and cropping and so on. At the point when the secret data is embedded, we can find the image block embedded secret data into as indicated by chaotic sequence and assurance the security of secret data embedded. This proposed model has high computation speed, bit variation and collision resistance and it is attempted on different cryptographic hash functions and hop based image steganography using extended dynamic chaotic map.

REFERENCES:

[1] Dr. D.S.R Murthy, B. Madhuravani," A HYBRID PARALLEL HASH MODEL BASED ON MULTI-CHAOTIC MAPS FOR MOBILE DATA SECURITY ", Journal of Theoretical and Applied Information Technology.

[2] Xiaoyun Wang and Hongbo Yu, How to Break MD5 and Other Hash Functions, EUROCRYPT, pp. 19-35, 2005.

[3] Xiaoyun Wang, Xuejia Lai, Dengguo Feng, Hui Chen, and Xiuyuan Yu, Cryptanalysis of the Hash Functions MD4 and RIPEMD, EUROCRYPT, pp. 1-18, 2005.

[4] Xiaoyun Wang, Yiqun Lisa Yin, and Hongbo Yu, Finding Collisions in the Full SHA-1, CRYPTO, pp. 17-36, 2005.

[5] N. Abdoun, S. El Assad, Md. A. Taha, R. Assaf, O. Deforges and Md. Khalil, "Hash Function Based on Efficient Chaotic Neural Network", "10th International Conference for Internet Technology and Secured Transactions", 2015.

[6] W. Guo, X. Wang, D. Hea and Y. Cao, "Cryptanalysis on a parallel keyed hash function based on chaotic maps", "Physics Letters A, 373(36)", pp.3201-3206, 2009.

[7] N. S. Raghava1, Ashish Kumar, Aishwarya Deep and Abhilasha Chahal, "Improved LSB method for Image Steganography using H´enon Chaotic Map", open journal of information security and applications volume 1, number 1, june 2014.

[8] Meysam Asgari Chenaghlu ∗, Shahram Jamali, Narjes Nikzad Khasmakhi," A novel keyed parallel hashing scheme based on a new chaotic system", Chaos, Solitons and Fractals 87 (2016)216–225.

[9] B Madhuravani, DSR Murthy, "Cryptographic Hash Functions: SHA Family", International Journal of Innovative Technology and Exploring Engineering (IJITEE).

[10] L. Gao, X. Wang and W. Zhang, "Chaotic hash function based on Tandem-DM construction", "International Joint Conference of IEEE TrustCom-11",2011.

[11] Neil F. Johnson, Sushil Jajodia, "Exploring Steganography: Seeing the Unseen", IEEE, Feb1998, pp. 26-34.

[12] B. Madhuravani, Dr. P. Bhaskara Reddy, "An Efficient Authentication Protocol to amplify collision resistance using Dynamic Cryptographic Hash Function & LSB Hop based Image Steganographic Technique", International Journal of Applied Engineering Research ISSN 09734562 Volume 11, Number 7 (2016) pp 5293-5296. Research India Publications. http://www.ripublication.com.

[13] B.Madhuravani, Dr. D.S.R. Murthy, Dr. P. Bhaskara Reddy, Dr. KVSN Rama Rao "Strong Authentication Using Dynamic Hashing And Steganography", Track 5 PgNos. 732735. Year of Publication 2015, ISBN:9781479988907/15& Conference Name: IEEE Inter National Conference on Computing, Communication and Automation [ICCCA2015].

[14] B. Madhuravani, D. S. R. Murthy, P. Bhaskara Reddy, "novel authentication protocol using multi cryptographic hashfunctions and Steganography", International Journal of Advanced Computing (IJAC), Vol. 48, May 2015.