Journal of Theoretical and Applied Information Technology
15th February 2017. Vol.95. No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A HYBRID PARALLEL HASH MODEL BASED ON MULTI-CHAOTIC MAPS FOR MOBILE DATA SECURITY

[1]B. MADHURAVANI, [2]Dr. D.S.R MURTHY

[1] Department of Computer Science & Engineering, MLR Institute of Technology, Dundigal, Hyderabad, Telangana, India

[2]Professor., Department of Computer Science & Engineering, Geethanjali College of Engineering & Technology, Keesara, Hyderabad, Telangana, India

E-mail: [1]madhuravani.peddi@gmail.com, [2]dsrmurthy.1406@gmail.com

ABSTRACT

Today, with the advancement of internet and technology security of information has become the prime concern in mobile and online applications. Extensive amount of research have been carried out since years to provide secure and reliable hash functions for information interchange. Chaos based hash functions have gained a lot of attraction by the researchers due to its non-linearity, randomness and unpredictable results. Various chaotic based hash functions have been implemented in the past decade to achieve confidentiality, integrity and authentication. But, most of the traditional chaos based hash functions are processed in sequential approach with a single dimensional map, which restricts their execution speed and performance in the mobile computing applications. To overcome these problems, a novel parallel chaotic hashing model is proposed in this paper. This model integrates multiple chaotic maps as a single chaotic system to generate an n-bit hash value for a given input message. This model provides more security, high computation speed, limit memory resources and less computation overhead in the standalone and mobile applications. Experimental results show that proposed model has high computational speed, bit variation and collision resistance as compared to traditional parallel chaotic models.

Keywords: *Parallel chaotic , Hash fucntion, Mobile computing, Integrity, Authentication*

1. INTRODUCTION

Message digest is a significant cryptographic algorithm which has its application in digital signature authentication, message authentication code, digital steganography, digital time stamping and, so on. In the year 1995, National Institute of Standards and Technology introduced this algorithm. Later various research efforts are made to integrate SHA with other approaches to achieve extended security and integrity. Hash function accepts variable-length message as input string and produces fixed-length digest as output after processing. SHA cannot prevent attacks and collisions of hash values which are the major problem of this algorithm. These algorithms are not very efficient for mobile applications which are dynamic in nature. SHA is also categorized into different algorithms- SHA, MD5 etc. Similar to other hash functions, SHA comes up with the message having arbitrary input length but a digest of fixed length. The original messages are converted into blocks of small fixed sizes.

For ensuring the integrity and authenticity, most of the digital applications such as digital documents, electronic mail, office automation, and electronic funds transfer were implemented using message digest as a security parameter. Hash functions are used as the basic component in various security protocols like TLS, SSL, and S-MIME. Also, hash function is regarded as the core part of digital signature and has gained a lot of attention amongst the various researchers.

Chaos based hash functions have gained a lot of attraction by the researchers in the field of cloud computing and mobile computing. Due to the limited computing power, chaotic orbits will become non-periodic. Most of the traditional chaos based hash functions are processed in sequential model, which restricts their execution speed and performance on the mobile computing. In [2] a parallel keyed hash function using the chaos-based algorithm is proposed. The limitations in the parallel chaos model were presented in [3]. Various experimental results have been performed on arbitrary messages and finally concluded that the parallel chaotic hash function is not secured against the statistical attacks.

To overcome this problem, complex chaotic-based hashing techniques are developed which are non-linear, random and dynamic in nature. It can be represented by either discrete or continuous systems. Henon mapping and logistic mapping can be categorized under discrete, whereas Lorenz and Rossler system comes under continuous. This system is highly responsive to initial conditions. Lyapunov exponents are one of the important components of chaotic system which decides whether the given system is chaotic or not. Our proposed scheme involves various logical functions and is developed according to the complex temporal behavior and provides high sensitivity to the initial constraints of the high-dimensional chaotic maps.

The main objective of a chaotic-hashing system is the convergence property in the complex chaotic systems. The features responsible for this convergence are:- a) Both are deterministic. b) Both are complex and not predictable. c) In chaotic system, a small change in the initial conditions can affect and reflect a huge change in the output. Similarly, in hashing a minor change in the key or plain text will modify the hashing output to a great extent. As convergence, there are some features responsible for divergence of these two areas of research. Those are:- a) Chaotic systems are represented by continuous spaces, but hashing is represented by discrete and finite spaces.

2. RELATED WORKS

Many efforts have been made by different researchers to merge chaotic theory with hashing mechanisms since years. Some of those works are mentioned below:-*N. Abdoun et.al*. implemented Chaotic Neural Network and developed an advanced secure hash algorithm [1]. They introduced a Chaotic Generator as the first part of their hash function and generated Neural Network parameters. The second part was termed as Chaotic Neural Network which is again categorized into input, output and hidden layer. Each layer is responsible for calculating a transfer function. The transfer function can be calculated by using the parameters provided by the Chaotic Generator. They validated their theory and proved that, their newly developed hash algorithm is collision resistant and has better statistical properties.

K. Atighehchi et.al. implemented considered hash tree approach in their research and developed a new parallel algorithm [2]. They emphasized on critical applications running on multi-core processors for optimized performances. Though their algorithm provides parallelism, it lacks a proper scheduling technique which can decrease the overhead.

K. Ganesan, et.al. implemented a previously existing algorithm for encryption using chaotic chebyshev maps [3]. They encrypted texts and performed cryptanalysis for backup and recovery purpose. The authors proposed an extended hashing technique for added security. In order to encrypt multimedia data, they used both hashing and scrambling techniques. They showed that, their technique added extended robustness and security.

L. Gao, X. et.al. analyzed the drawbacks of traditional hashing technique like the need of vast amount of resources [4]. In order to overcome this problem, they integrated Discretized Chaotic Map Network (DCMN) with Tandem-DM. Their function uses integer fields instead of using floating points. They simulated their theory and got better efficiency and collision resistance than that of conventional algorithm.

W. Ghonaim, et.al. implemented an advanced version of chaotic hashing technique and implemented that in Parallel Chaotic Neural Networks [5]. Their proposed function is collision resistant and gives better performance, as proved by simulation results. The researchers also stated a new type of attack and termed it as Semi-Collision attack. Their introduced method is prone to the above said attack. Therefore, further research is necessary to prevent this attack.

R. Guesmi et.al. implemented a new algorithm to encrypt image data by merging DNA masking, SHA-2 and Lorenz system [6]. One of the most important pros of this approach is better information entropy. The authors validated their work and demonstrated that their approach is secure from statistical and exhaustive attacks. Most useful application of this technique is digital image encryption.

W. Guo, et.al. carried out their research on parallel computing to achieve better efficiency [7]. They experimented on chaotic-based hashing technique with parallel keys. This approach was introduced by *Xiao*. The authors tried to prevent forgery attack on the above said approach by the method of differential cryptanalysis. With their experiment they also proved that weak keys are responsible for collision which added a major drawback to this technique.

To add increase security *[8]* merged chaotic function with OTP scheme and developed a new algorithm which is able to prevent attacks [8]. By using chaotic scramble-sort algorithm and Henon-mapping chaotic hashing, they formed the above said One Time Password. Their proposed approach contains all the advantages of chaotic hashing along with the additional security of new OTP technique.

W. Jizhi, et.al. made a thorough survey on chaotic one-way hashing schemes and found absence of proper mapping technique [9]. They also stated that the hash values may collide with each other, if a wrong mapping technique is encountered. The authors proposed a non-linear mapping and validated that through experimental analysis. Their approach solves an important problem i.e., poor diffusion.

Y. Li, D. Xiao, et.al. presented parallel chaotic hashing based on 4-D Cellular Neural-Network [10]. They divided their whole process into four steps- Message expansion, followed by parameters utilization, followed by parallel processing and hash value generation. The authors validated their work and resulted better performance and security than that of conventional hashing.

M. Nouri, A et.al. introduced a dynamic hashing scheme combined with chaotic mapping [11]. Along with all features of chaotic system, their algorithm also supports parallel processing. The index of message blocks produces parameters of above said algorithm dynamically, which ensures the dynamic nature of hashing technique. Better efficiency, collision resistant, controllable parameters, security against attacks are some of the advantages which are validated by the researchers through their experiments.

Y. Song et.al. presented a new methodology for hashing by using Chaotic Coupled Map Network [12]. This technique is responsible for transformation of variable-length message to fixed-sized hash. While experimenting they found that, their algorithm is highly responsive to initial values and coupled factor. As it has all the advantages of chaotic mapping, it can be applied in the secure digital signature scheme.

Y. Wang, et.al. used iterated-chaotic mapping technique to develop a new algorithm for one-way hashing [13]. They split the whole space and different chaotic sub-spaces were formed by using density distribution function. Each individual sub-divided space is represented by a unique bit. The chaotic value is calculated dynamically, whereas hash value is represented as bit sequence. The authors demonstrated that the proposed approach can prevent most of the attacks like birthday attack , statistical attack and man-in-the-middle attack.

Q. Zhang, et.al. proposed an algorithm using both one-way hashing and chaotic functions [14]. Variable-sized input strings are split into fixed-sized output and iterated by using standard mapping. The output of iteration calculates initial values and the next iterations. Output of the last iteration is converted to hash value. They simulated their approach and stated that, their proposed algorithm is collision resistant, irreversible and sensitive to initial values. To make this algorithm more secure, further work is needed to increase the length of hash value.

M. T. Mohammed, combined hashing with chaotic system and introduced a new technique, which is collision resistant and having better avalanche effects [15]. They implemented this algorithm using Lorenz system. The authors validated their theory through experiment and found that, their technique is more secure with good performance as compared to the conventional ones. Further works are needed to integrate this algorithm with various other security protocols.

P. Fei, et.al. implemented elliptic curves and chaotic system to develop a new digital signature algorithm [16]. They integrated one-way hashing, 2D hyper-chaotic mapping with public key algorithm to form their new approach. Their algorithm prevents duplicate signature key attack. As the proposed algorithm is reliable, secure and simple it can be implemented in practical scenarios. In this section we have thoroughly studied various works in the field of chaotic-based secure hash algorithms. We have analyzed and identified their objectives, empirical validations, pros and cons of each approach.

3. PROPOSED MODEL

Due to the non-linear features of dynamic chaotic systems, traditional chaotic maps such as quadratic-map, logistic with sine map, polynomial map have been widely applied in the real-time applications. In our work, we proposed a novel hashing model based on multi-chaotic system with parallel approach. The suggested model is fast and accurate in terms of speed and security is concern. In this model, multiple chaotic maps are integrated as a single chaotic system to generate an n-bit digest value for a given input text M, where n is

any 32-bit value, it is generally selected from the set of 128, 256, 512 and 1024 bit value.
In this section, we describe our model to multi-chaotic system that overcomes the issues of parallel chaotic systems. Traditional parallel chaotic systems failed to initialize the parameters to the chaotic maps. Also, initialization parameters are vulnerable to several well known attacks such as permutation, diffusion and statistical attacks.

Non-Linear Chaotic-Maps:

The non-linear chaotic map in the dynamic systems is represented as equation (1):

Controlled Chebyshev Chaotic Map:

Let n be a real integer x from the set G onto G such that ,

$$T_n(x): G->G:[-1,1]->[-1,1]$$

$$T_n = k\cos(n.\cos^{-1} x) \text{ --(1)}$$

The recurrence relation to the equation (1) is given as

$$T_n(v) = (vT_{n-1}(v) - T_{n-2}(v))/k$$

and

$$T_0(v) = k, T_1(v) = kv.$$

Extended Quadratic Map:

The non-linear quadratic map in the dynamic systems is given as equation (2):

$$X_{n+1} + kX^2{}_n = c \text{ ---(2)}$$

$$X_{n+1} = c - kX^2{}_n$$

Here, c values lies between 0 to 2. i.e $c \in (0,2)$ and $k \in (0,1)$.

Generally, chaotic map have areas on the plotted graph with split point known as Bifurcation. These split points occurs at fixed points such that

$$f(X_n) = X_n$$

In chaotic maps, one or more solutions are possible with attraction to the fixed point and repulsion from the fixed point. In case of attractive, the fixed point is stable, whereas in repulsive case all possible fixed points are unstable.

Case 1: if x is fixed .

$$kx^2 + x - c = 0$$

$$x_{+/-} = \frac{-1 \pm (1+4c)^{1/2}}{2k}$$

Since , fixed points exist in the neighborhood of the chaotic maps.

$$X_n = X_\pm + \Delta_n(x)$$

$$X_n = c - kX_n{}^2$$

$$X_{n+1} = c - k(X + \Delta_n(x))^2$$

$$X_{n+1} = c - k(X^2 + 2\Delta_n(x)X + (\Delta_n(x))^2)$$

$$X_{n+1} = c - k(X)^2 - 2.k\,\Delta_n(x)X - k(\Delta_n(x))^2$$

$$\text{we have } X_{n+1} = X + \Delta_{n+1} \text{ and } X = C\text{-}kX^2$$

$$X + \Delta_{n+1} = X\text{-}2.k\,\Delta_n(x)X - k(\Delta_n(x))^2$$

Since,sΔ_n is small factor,$\Delta_n(x))^2$ is even smaller, we have

$$\Delta_{n+1} = -2k\Delta_{n+1}(x)X \text{ ----(3)}$$

This equation gives the stability of x with respect to k.
Two possible solutions from the equation (3) include:
1) if $|\Delta_{n+1}|>|\Delta_n|$, there is a case of repulsion from x w.r.t k.
2) if $|\Delta_{n+1}|<|\Delta_n|$, there is a case of attraction towards x w.r.t k.

Extended DCS:

Traditional DCS(Dynamic chaotic system)[1] uses weighted parameters with the range 0 to 1.Also, existing DCS has uniform distribution over all the possible values of X_n and r, while two constant parameters are fixed as constant ($w_\alpha\alpha$ and $w_\beta\beta$).Since, r of DCS with logistic map is in the range of (0,16) ,the distribution of r with respect to X_n are easily predicted using the statistical and frequency attacks. To overcome these issues, we extended the traditional DCS[1] scheme with a non-linear chaotic map as a third parameter to improve the security in the mobile computing applications. In this extended model we used three weighted components α,β,γ within range (0,1] using the following equation (4).

$$EDCS = X_{n+1}(\alpha,\beta,\gamma) = w_\alpha\alpha(r.A\,X^2{}_n + w_\beta\beta(16-r).A\,X^2{}_n) + w_\gamma\gamma(\frac{(w_\alpha\alpha + w_\beta\beta)}{2})A\,X^2{}_n \text{ -----(4)}$$

Eq.4 follows non-linear quadric map with more chaotic and random as shown in Figure

Journal of Theoretical and Applied Information Technology
15th February 2017. Vol.95. No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

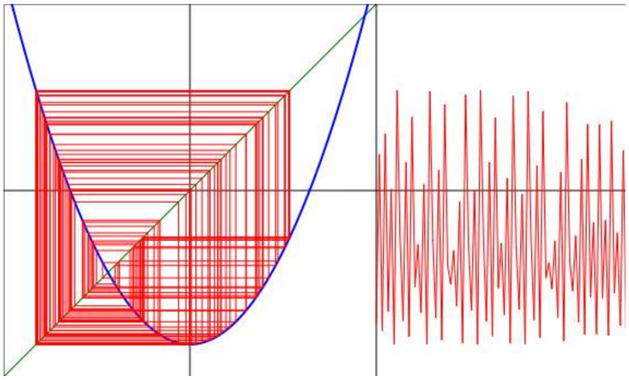

Figure 1: Bifurcation Of Non-Linear Chaotic Map

Figure 2, represents the proposed extended chaotic model with parallel approach implemented on arbitrary input messages. The input text message M is divided into chunks of n- blocks, ($B_1, B_2 .... B_n$), each with r-length. Append padding bits $(10000…00)_2$ with length 'q' at the end of the message M. After padding, each block is again divided into 'm' sub-blocks, each with 32-bit length and it is represented as $P_1, P_2 .... P_m$. Here, secret key is generated dynamically using the client mobile/PC's processor-id. In this system, we have introduced an extended multi-chaotic system with three maps: Controlled Chebyshev Chaotic Map, Extended Quadratic Map and Extended DCS. In each round function, iterative multi-chaotic system generates output to the transformation box.

In the transformation box, input sub-blocks , chaotic output and scaling value are used to perform XOR operation and then permutate operation. Permutate operation divides the input XOR value into four 8-bit blocks to generate hash value as shown in figure 3.

The permute function in the figure 3, consists of logical operations such as rotate function, XOR and circular shift operations using hardware secret key.To improve the security and bit variation, the shift operations are performed are dependent on each bit sequence and kth processing iteration. The output of the each iteration is fed as the input to the next iteration. The overall pseudo code steps are summarized as follows:

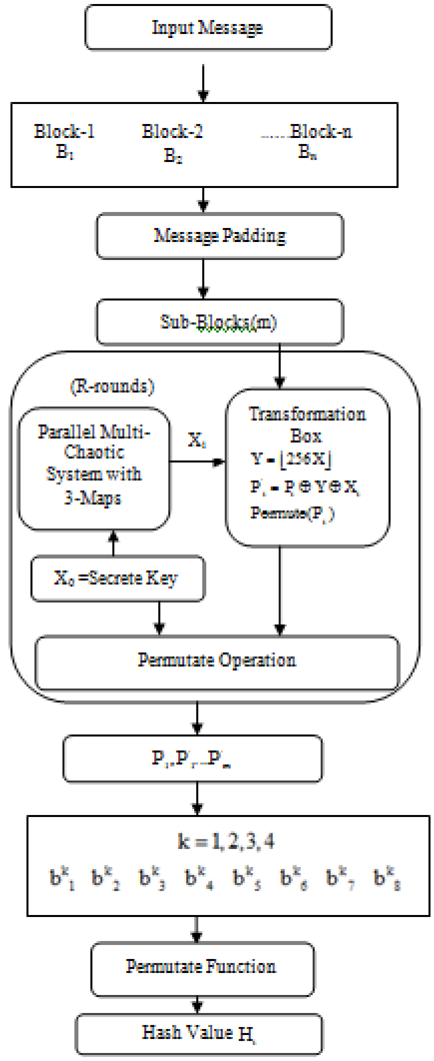

Figure 2: Proposed Parallel Multi-Chaotic Model

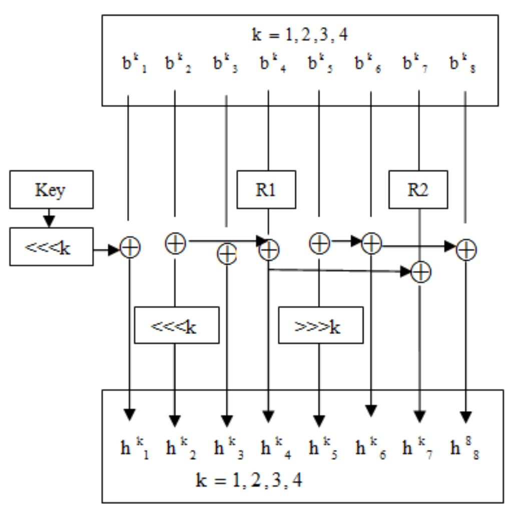

Figure 3: Permute Function

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Algorithm Steps:

Input: M(Input message),Secret key, initialization parameters.

Step 1: Read a message M .

If message size is not multiple of 'n' then

Append the bit sequence 1000…000 at the end of the message.

Step 2: Divide the message into blocks of length n as $B_1, B_2 .... B_n$.

Step 3: After padding, each block is again divided into 'm' sub-blocks, each with 32-bit length and it is represented as $P_1, P_2 .... P_m$.

Step 4: Secret key is generated using the client's mobile/PC processor-id as S. Generated secret key is initialized as X_0 for multi-chaotic system.

Step 5: Extended multi-chaotic system with three maps:Controlled Chebyshev Chaotic Map, Extended Quadratic Map and Extended DCS are used using equation (1), (3),and (4).

Step 6: In each round function, iterative multi-chaotic system generates output X_i to the transformation box as shown in Figures 4,5,6.

$$X_i = C_1 \oplus C_2 \oplus C_3$$

Step 7: In the transformation box, the following operations are performed on the Y and chaotic output.

$$Y = \lfloor 256X \rfloor$$

$$P'_i = P_i \oplus Y \oplus X_i$$

$$\text{Permute}(P'_i)$$

Step 8: Generates Hash value as

$$H_i = \text{Permute}(P'_i)$$

$$\text{Hash} = H_1 + H_2 + H_3 .... H_m$$

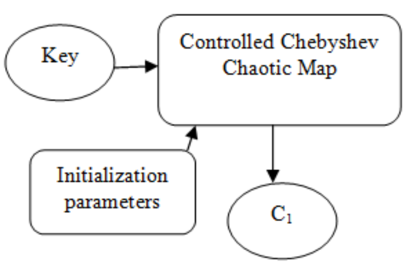

Figure 4: Controlled Chebyshev Chaotic Map Operation

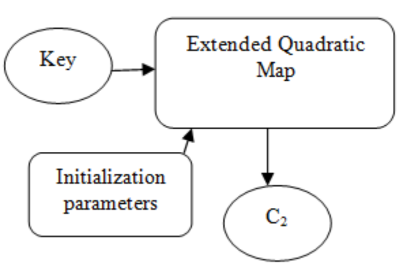

Figure 5: Extended Quadratic Map Operation

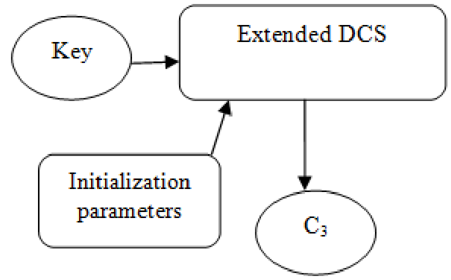

Figure 6: Extended DCS Operation

4. EXPERIMENTAL RESULTS

In this section, we perform different experiments to find the efficiency 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.

Hash Sensitivity:

Hash sensitivity of the input message to the changed message are evaluated using different conditions. Experimental results demonstrate the high sensitivity of the original to the changed one in different cases.

Experimental-1: Proposed Model Vs Kanso [15]

Original Message: This is a message for testing !!

Hash Value
a54cc13a7c81f87e5f205944f19356210efb5675e4ff ea724ef6b803105efc16

Binary Value
0011100000000100001011101111000111011010101101011011000101010101000111001110100100100111101111000011010011110111111100000111101010101100001111111100010101111110111111101011001010010100101111101110010100111101011111001010101000110110011110000011100 1111010011

T-1: This is a message for testing !?

Hash Value
:89516b01e790ddd4f14cc6529d6c8be8a7817a4c82 d543086bf6018521c42b77

Binary Value
:1011000101011001001101101110001001010010111110111011111101111110110010001001111010001001001010101111010010000011011010110001110111111111111111111011110000101100010111111110110000011010100111010110100001100011001111110001101000101001101001101000101100010100100

Proposed Bit Change:140

Kanso Bit Change: 132

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

T-2: Thes is a message for testing !!
Hash Value
:d9eb62ec69b136c7f2dcec4282080f0fd7c31fcb2090dec4642fa512ce58b392
Binary Value
:1110000111100011001111110000111111011100110110100101010001101101110010110000111010100011001110101110101111100111111011111111110101000111110111100100101010011011011011101111110101111101111011100110101110010101010101011100010001101010001010101000110000 0001000001
Proposed Bit Change:146
Kanso Bit Change:131

T-3: This is a message for tsting !!
Hash Value
:f97ac3d75034d5b4351a73c61abd4b08cc3ad0a03e4a5805df075d36424adc24
Binary Value
:110000010111001010011110001101001110010101011111110110111000111100000110011001000001111001011111001110011010100101010101111111101100101000100010101011010010111011100001100101111011100010111100000010101011111011010010001100010001011101011101010101 1 1111110111
Proposed Bit Change:140
Kanso Bit Change:128

T-4: This is a message for tsting !!
Hash Value
:cad52e03e2feced38321e9004a18773ae970cdd2a2d10e37bbd31673616793b5
Binary Value
:111100101101110101110011111000000101011110010101101011000111100110111010111100111010011001111100000100011111101111001011111001111101100010000011110100011100101111010111111011010000100111010010100111000110101001111011111001001110000011011001011111110000001100110
Proposed Bit Change:145
Kanso Bit Change:135

Experimental-2: Proposed Model Vs [16]

Original Message: The quick brown fox jumps over the lazy dog.
Hash Value:
be412c4af3b1f7a3b29bde63db5d98e139dc3d1d083fcffb7e9d195e9c2d5b96
Binary Value:
1000011001001001011100011010100101000110110110101001010100001001100010110100100110010001000110111011001010110010011110000001010001100001101000111011011111000001111010101011010111001101000011010110100111001111110000000001010111100001101110100101000 01000101

T-1: The quick brown fox jumps over the lazy dog,
Hash Value
:e5bf884791614cd17938e90e4feac752d966749cfa91552b7d33b77f10c711aa
Binary Value
:0110001111110110111111001111011101101011110111011111011001110110001111001001110001011110000000101011111110101011000101111110100011010111000110001011100001101111100000011111110010111011001110101101110010011101010001010111011101011110000000011010001110 0111101111
Proposed Bit Change:150
Chenaghlu[16] Bit change:138

T-2: the quick brown fox jumps over the lazy dog.
Hash Value
:ccdf6c1978e17263e99a95ef0c1c8b22ef13d82bc9b453398d07125b1881b499
Binary Value
:0100101010010110000111011011000000111110001110111110011101101010011000101101001100000100111101001011111010101110111100110011011010001110101100000110111111001011001111001110111010110101101111110011100111100000111100100101000111101000010111001001110011011100
Proposed Bit Change:141
Chenaghlu[16] Bit change:114

T-3: The quick brown fOx jumps over the lazy dog.
Hash Value
:b2e2c2bd70cbf96cff307333de8c0ae3744e14afa1a25fbd79617dd967b0d4b8
Binary Value
:0011010010101011101100110001010000110110000100010110110001100101011101000111100111100010001010000110110000111110011100101111011110001010111101101101000110100111101010100111110001011100100111011110011011000011101001110111010011100101110110110111111100 11111101
Proposed Bit Change:141
Chenaghlu[16] Bit change:130

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

T-4: The quick brown fox jumps over the laZy dog.
Hash Value
:b2e2c2bd70cbf96cff307333de8c0ae3744e14afa1a
25fbd79617dd967b0d4b8
Binary Value
:00110100101010111011001100010100001101100
00100010110110001100101011101000111100111
10001000101000011011000011111001110010111
10111000101011110110110100011010011110101
01001111100010111001001110111100110110000
11010011101110100111001011101101101111111
0011111101
Proposed Bit Change:141
Chenaghlu[16] Bit change:135

T-5: The quick brown fox jumps over the lazy dog
Hash Value
ba86e448c62113e616f42759fd5fffc78d7c2c061a6a
4129f46a726f93dcf228
Binary Value
:00111100110011111001010111100001100000001
11110111000011011101111100111011011110110
11011001000010010011111110110110000111110
10011111011001101111110011011111001101110
11110011000010100111101011110100000010001
10110010010011001010110001100000001110110
1001101101
Proposed Bit Change:143
Chenaghlu[16] Bit change:131

From the above two experimental results , it is clear that any change in the original message has a huge impact on the final output. From these experimental results, we conclude that our proposed model has high hash sensitivity compared to traditional models[15][16].

Table 1: *Statistical analysis of "yahoonews" text datasets using proposed model*

	Number of Samples			
	256	512	1024	2048
B(min)	115	108	118	113
Avg(B)	135.75	132.87	136.75	131.87

5. CONCLUSION

In this paper, a novel parallel chaotic hashing model is analyzed with experimental results; whose structure can ensure the randomness, high sensitivity and collision resistance. This model integrates multiple chaotic maps as a single chaotic system to generate an n-bit hash value for a given input message. This model provides more security, high computation speed, limit memory resources and less computation overhead in the standalone and mobile applications. Experimental results show that proposed model has high computational speed, bit variation and collision resistance as compared to traditional parallel chaotic models. In future, this work can be extended to encryption based chaotic model on mobile devices.

REFRENCES:

[1] 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.

[2] K. Atighehchi and T. Muntean, "Generic Parallel Cryptography for Hashing Schemes", "IEEE 12th International Symposium on Parallel and Distributed Computing", 2013.

[3] K. Ganesan, I. Singh and M. Narain, "Public Key Encryption of Images and Videos in Real Time Using Chebyshev Maps", "5th International Conference on Computer Graphics, Imaging and Visualization", 2008.

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

[5] W. Ghonaim, N. I. Ghali, A. E. Hassanien and S. Banerjee, "An improvement of chaos-based hash function in cryptanalysis approach: An experience with chaotic neural networks and semi-collision attack", "Memetic Computing", 5(3), pp.179-185, 2013.

[6] R. Guesmi , M. A. B. Farah, A. Kachouri and M. Samet, "A novel chaos-based image encryption using DNA sequence operation and Secure Hash Algorithm SHA-2", "Nonlinear Dynamics", pp. 1123-1136, 2016.

[7] 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.

[8] N. Jiang, R. Yang and X. Liu, "The Design and Implementation of Password authentication System Based on chaos", "International Workshop on Chaos-Fractals Theories and Applications", 2009.

[9] W. Jizhi, X. Shujiang, T. Min and W. Yinglong, "The analysis for a chaos-based one-way hash algorithm", "International Conference on Electrical and Control Engineering", 2010.

[10] Y. Li, D. Xiao, H. Li and S. Deng, "Parallel chaotic Hash function construction based on

cellular neural network", "Neural Computing and Applications 21.7", pp.1563-1573, 2012.

[11] M. Nouri, A. Khezeli, A. Ramezani and A. Ebrahimi, "A Dynamic Chaotic Hash Function Based upon Circle Chord Methods", "6th International Symposium on Telecommunications", 2012.

[12] Y. Song and G. Jiang, "Hash Function Construction Based on Chaotic Coupled Map Network", "IEEE 9th International Conference for Young Computer Scientists", 2008.

[13] Y. Wang, D. Yang, M. Du and H. Yang, "One-way Hash function construction based on iterating a chaotic map", International Conference on Computational Intelligence and Security Workshops", 2007.

[14] Q. Zhang, H. Zhang and Z. Li, "One-way Hash Function Construction Based on Conservative Chaotic Systems", "5th International Conference on Information Assurance and Security", 2009.

[15] A. Kanso, H. Yahyaoui, M. Almulla," Keyed hash function based on a chaotic map"," Information Sciences 186 (2012) 249–264.

[16] 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.

[17] B. Madhuravani, Dr. DSR Murthy, "An Efficient Authentication Protocol to amplify collision resistance using Dynamic Cryptographic Hash Function & LSB Hop based Image Stegano-graphic Technique", International Journal of Applied Engineering Research ISSN 0973-4562 Volume 11, Number 7 (2016) pp 5293-5296. Research India Publications. http://www.ripublication.com.

[18] 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.

[19] 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. 732-735. Year of Publication 2015, ISBN:978-1- 4799-8890-7/15& Conference Name: IEEE Inter National Conference on Computing, Communication and Automation [ICCCA 2015].