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

B. MADHURAVANI, Dr. D.S.R MURTHY

1 Department of Computer Science & Engineering, MLR Institute of Technology, Dundigal, Hyderabad, Telangana, India
2Professor., Department of Computer Science & Engineering, Geethanjali College of Engineering & Technology, Keesara, Hyderabad, Telangana, India
E-mail: 1madhuravani.peddi@gmail.com, 2dsrmurthy.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 function, 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. Atighechhi 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 the last 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
Non-Linear Chaotic-Maps:

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

\[ T_n(x) : G \to G : [-1,1] \to [-1,1] \]

\[ T_n = k \cos(n \cos x) \] ---(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):

\[ X_{n+1} + kX_n^2 = c \] ---(2)

\[ X_{n+1} = c - kX_n^2 \]

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.

\[ X_n = X_2 + \Delta_n(x) \]

\[ X_n = c - kX_n^2 \]

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

\[ X_{n+1} = -2kX_n^2 - k \]

\[ X_{n+1} = X_{n-1} + \Delta_n \]

we have \[ X_{n+1} = X + \Delta_n \]

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

\[ \Delta_{n+1} = -2k\Delta_n(x)X \] ----(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 \( (w_\alpha, w_\beta) \). 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 \( \alpha, \beta, \gamma \) within range \((0, 1)\) using the following equation (4).

\[ \text{EDCS} = X_{n+1}(\alpha, \beta, \gamma) = w_\alpha X_n^2 + w_\beta (16 - r).AX^2 + w_\gamma \frac{(w_\alpha + w_\beta)(X^2 - X)}{2} \] ----(4)

Eq.4 follows non-linear quadric map with more chaotic and random as shown in Figure.
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 \((10000...00)\) 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 permute operation. Permute 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 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:
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.

\[ Y = [256X] \]
\[ P_i = P_i \oplus Y \oplus X_i \]
\[ \text{Permute}(P_i) \]

Step 8: Generates Hash value as

\[ H_i = \text{Permute}(P_i) \]
\[ \text{Hash} = H_1 + H_2 + H_3,...H_m \]

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:
00111000000100001011101100111001110011010101
10101101000010000101000001000100001000100001
010110110100010100110000101100110000100100
010110110100010100110000101100110000100100
111111010100100010100001011001000010001000
111111010100100010100001011001000010001000
010110110100010100110000101100110000100100
111111010100100010100001011001000010001000

Proposed Bit Change: 140
Kanso Bit Change: 140

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

Hash Value: 89516b01e790ddd4f14cc6529d6c8be8a7817a4c16df543086bf6018521c42b77

Binary Value:
01111000000100001011101100111001110011010101
10101101000010000101000001000100001000100001
010110110100010100110000101100110000100100
010110110100010100110000101100110000100100
111111010100100010100001011001000010001000
111111010100100010100001011001000010001000
010110110100010100110000101100110000100100
111111010100100010100001011001000010001000

Proposed Bit Change: 140
Kanso Bit Change: 132
T-2: This is a message for testing !!

Hash Value:
\(:d9eb62ec69b136c7f2dceec4282080f0fd7c31fcb209\)

Binary Value:
\(:\text{01101000111000111001111000011111111101111001}\)

Proposed Bit Change: 146

Kanso Bit Change: 131

T-3: This is a message for testing !!

Hash Value:
\(:f97ac3d75034d5b4351a73c61abd4b08cc3ad0a03e4a5805df075d36424adc24\)

Binary Value:
\(:\text{01100001011100101001111000110100111001010}\)

Proposed Bit Change: 140

Kanso Bit Change: 135

T-4: This is a message for testing !!

Hash Value:
\(:\text{cad52e3c2feced38321e9004a18773ae970cdd2a2d10e377bd31673616793b5}\)

Binary Value:
\(:\text{011100101100010100010000110011101111011001}\)

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:
\(:\text{be412c4a3f3f17a3b29bde63db5d98e139dc3d1d083fcff7e9d195e9c2d5b96}\)

Binary Value:
\(:\text{00010000010101001001010001010000110010100111}\)

Proposed Bit Change: 141

Chenaghlu[16] Bit change: 130
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 parallel chaotic models. In future, this work can be extended to encryption based chaotic model on mobile devices.

### Table 1: Statistical analysis of “yahoonews” text datasets using proposed model

<table>
<thead>
<tr>
<th>Number of Samples</th>
<th>256</th>
<th>512</th>
<th>1024</th>
<th>2048</th>
</tr>
</thead>
<tbody>
<tr>
<td>B(min)</td>
<td>115</td>
<td>108</td>
<td>118</td>
<td>113</td>
</tr>
<tr>
<td>Avg(B)</td>
<td>135.75</td>
<td>132.87</td>
<td>136.75</td>
<td>131.87</td>
</tr>
</tbody>
</table>

**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.

### REFERENCES:


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


