Robust Chaos Via Dome Logarithmic Map

Fadi Abu-Amara
Computer & Information Science Department, Higher Colleges of Technology
P.O. Box: 41012, Abu Dhabi, UAE

Salam A. Hoshang
Computer & Information Science Department, Higher Colleges of Technology
P.O. Box: 41012, Abu Dhabi, UAE

Abstract—Many chaotic maps have been developed and used to encrypt digital images. The small key space of those chaotic maps lowers the security of image encryption schemes. In this paper, one-dimensional chaotic map, referred to as Dome Logarithmic Map, is proposed. The Dome Logarithmic Map is utilized to develop an image encryption scheme that consists of three phases. First, an image is divided into square blocks. Second, pixel locations of each block are shuffled. Finally, pixel intensity values are modified based on the Dome Logarithmic Map. Experimental results indicate that the Dome Logarithmic Map achieves the S-unimodality property, has high sensitivity to a minor change in initial conditions, pose bifurcation within an interval, and has chaotic behavior. Results also indicate the proposed image encryption scheme has great substitution and permutation of original image content.

Keywords—Chaotic Map, Image Encryption, Lyapunov Exponent, Bifurcation Diagram, S-unimodality.

I. INTRODUCTION

The quick development of technology increased the demand for storage and transmission of digital images. In this regard, contemporary issues, such as distribution and illegal copying of digital documents, arise. One of the solutions to such problem is the use of image encryption techniques which intended to protect against illegal release of confidential documents to unauthorized persons and protect people’s privacy. The literature reported different chaotic algorithms such as two sets of one-dimensional Logistic mappings [1], N-phase Logistic Chaotic Sequence [2], bit-level Arnold Transform and Hyper chaotic maps [3], and Ikeda and Henon chaotic maps [4]; to name a few. Unfortunately, the small key space of the proposed chaotic maps lowers the security of the image encryption schemes developed based on these chaotic maps [1].

In this paper, the Dome Logarithmic Map (DLM) is proposed as a one-dimensional chaotic map to meet the need for a large key space. The S-unimodality property, high sensitivity to a minor change in initial conditions, bifurcation within an interval, and chaotic behavior characteristics of the DLM are investigated. Based on the DLM, an image encryption scheme is proposed that consists of three phases. The first phase is intended to divide the original image into square blocks. The second phase is intended to shuffle pixel locations of each block while the third phase is intended to modify pixel intensity values of each block.

The rest of this paper is organized as follows. Section
II introduce the proposed Dome Logarithmic Map. Section III investigates characteristics of DLM while Section IV explores the proposed DLM-based image encryption scheme. Section V analyze experimental results while Section VI concludes the paper.

II. DOM LOGARITHMIC MAP

The proposed Dome Logarithmic Map is characterized by

$$x_{n+1} = \begin{cases} \frac{\lambda + \ln(\lambda x_n + 0.21)}{\lambda}, & 0 \leq x_n \leq 0.5 \\ \frac{\lambda + \ln(\lambda(1-x_n) + 0.21)}{\lambda}, & 0.5 < x_n < 1 \end{cases}$$

(1)

where $x_{n+1} = DLM(x_n, \lambda)$ is the iteration function satisfying the condition $DLM:[0,1] \rightarrow [0,1]$. The two control parameters of the Dome-Logarithmic Map are $\lambda$ and the initial value $x_0$.

III. DLM CHARACTERISTICS INVESTIGATION

This section investigates characteristics of the proposed Dome Logarithmic Map. The investigated characteristics are S-unimodality, sensitivity to a minor change in initial conditions, bifurcation within an interval, and chaotic behavior.

The iteration function of DLM is shown in Fig. 1 for $\lambda = 1.567$ and for $\forall x_0 \in [0,1]$. Fig. 1 shows a unimodal function that has a single critical point at $x = 0.5$, start from 0 and keeps increasing until it reaches its maximum value and then decreases back to 0.

Another characteristic to investigate is the high sensitivity to initial conditions. Fig. 2 shows time series plot of 100 DLM iterations obtained for two different initial conditions; $x_0 = 0.322$ and $x_0 = 0.32201$

As shown in Fig. 2, the two sequences are different after a few iterations which indicate the high sensitivity to a minor change in initial condition value.

The DLM should pose the bifurcation within an interval characteristic. The Schwarzian Derivative is used to study the bifurcation characteristic as shown in Equation 2 [5]. Fig. 3 shows the obtained Schwarzian Derivative plot for one hundred iterations using the parameters $\lambda = 1.567$ and $x_0 = 0.322$. As the figure shows, a negative Schwarzian Derivative is generated which indicates the robust chaos provided by the proposed DLM.

On the other hand, the Bifurcation Diagram is used to find range of the parameter $\lambda$ within which the DLM achieves the unimodality property. The Bifurcation Diagram displays all possible ranges of the control parameter $\lambda$ that may result in unimodal DLM. Fig. 4 shows the Bifurcation Diagram of DLM. As Figure indicates, the DLM achieves the unimodality property for control parameter range $\lambda \in [1.5329,1.5944]$.

![Fig. 1 The iteration function of DLM for $\lambda = 1.567$](image1)

![Fig. 2 Time series plot of 100 DLM iterations for two](image2)
sequences generated; blue \((x_0 = 0.322)\) and red \((x_0 = 0.32201)\) lines; respectively

\[
S_f(x) = \int \frac{f'(x)}{f(x)} - 1.5 \left( \frac{f'(x)}{f(x)} \right)^2
\tag{2}
\]

Another method used to investigate the chaotic behavior of DLM is the Lyapunov Exponent that determine the unstable orbits, that result in chaotic behavior, and the periodic orbits that result in non-chaotic behavior \[5\]. The Lyapunov exponent is defined by

\[
\lambda_{LE}(x_0) = \lim_{N \to \infty} \frac{1}{N} \sum_{n=0}^{N-1} \ln|f'(\lambda, x_n)|
\tag{3}
\]

\[
 f'(x_n, \lambda) = \begin{cases} 
 1, & 0 \leq x < 0.5 \\
 \frac{1}{0.21 - \lambda(1-x_n)}, & 0.5 \leq x \leq 1 
\end{cases}
\tag{4}
\]

where \(f'(0.5, \lambda)\) is undefined. Fig. 5 shows the graphed Lyapunov Exponent of the DLM for \(\lambda \in [1, 2.2]\). A chaotic behavior is obtained for \(0 < \lambda_{LE} \leq \ln 2\). As the figure shows, the DLM exhibits chaotic behavior for \(\lambda \in [1.24892, 2.0116]\).

Through combining the results of Bifurcation Diagram and the Lyapunov Exponent, the proposed Dome-Logarithmic Map provides robust chaos and achieves the S-unimodality property for \(\lambda \in [1.53291, 5.944]\). In comparison, the Tent Map and the Logistic Map offer robust chaos and achieves the S-unimodality property for \(\lambda \in [1.9992]\) and \(\lambda \in [3.694]\); respectively \[6\]. Thus, the DLM has a large key space.

\[
\begin{align*}
\text{Fig. 3} & \quad \text{The Schwarzian derivative of DLM} \\
\text{Fig. 4} & \quad \text{The Bifurcation Diagram of DLM in the range } \lambda \in [1, 2.2] \\
\text{Fig. 5} & \quad \text{The Lyapunov exponent of the DLM for } \lambda \in [1, 2.2] 
\end{align*}
\]

**PROPOSED DLM-BASED IMAGE ENCRYPTION SCHEME**

The Dome-Logarithmic Map is utilized to develop an image encryption scheme. The original image, of size 300 \(\times\) 300 pixels, is divided into square blocks; each block is of size 15 \(\times\) 15 pixels. For each square block, the following steps are performed:
- The block is converted into row vector of size $1 \times 225$ pixels.
- Pixel locations of the corresponding row vector are randomly shuffled.
- Pixel intensity values of the shuffled row vector are modified using the bitwise exclusive OR per:
  \[ B_e = B_s \oplus K \]  
  \( (5) \)
  where $B_s$ represents the shuffled row vector from the previous step and $K$ is constructed according to Equation 1 using the secret key parameters $x_0 = 0.25, \lambda = 1.567$.
- The encrypted row vector is converted into square block of size $15 \times 15$ pixels.
- The encrypted image is constructed from the encrypted blocks.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

Fig. 6 shows the original $300 \times 300$ pixels Lena test image while Fig. 7 shows its histogram. The encrypted image is obtained for secret key parameters $x_0 = 0.25, \lambda = 1.567$ as illustrated in Fig. 8. As Fig. 8 shows, a complete obscuring of original image content is obtained using the proposed image encryption scheme. As Fig. 9 shows, the encrypted image has a semi-uniform histogram indicating the greater substitution and permutation properties of the proposed scheme making it immune against histogram attack methods.

CONCLUSION AND FUTURE WORK

A one-dimensional chaotic map, referred to as Dome Logarithmic Map, is proposed in this paper. Characteristics investigation indicated the DLM pose interesting characteristics such as large key space, $S$-unimodality, high sensitivity to initial conditions, robust chaos, and full chaotic behavior. Based on the DLM, an image encryption scheme is proposed that divided image into blocks, shuffle content of each block, and modify the content of each block. Experimental results indicate a great substitution and permutation of original image content. Future work should investigate methods to reduce the
computational complexity of the image encryption scheme to decrease encryption time without compromising the encryption security.

Fig. 9 Histogram of the encrypted image

REFERENCES


