Image Encryption Based on Double-Humped and Delayed Logistic Maps for Biomedical Applications


aFaculty of IET, German University in Cairo (GUC), Egypt.
bNISC Research Center, Nile University, Cairo, Egypt.
cDept. of Engineering Mathematics and Physics, Cairo University, Egypt.
dRadiation Engineering Dept., NCRRT, Egyptian Atomic Energy, Authority.
eElectronics and comm. Eng. Dept., Cairo University, Egypt.

Abstract—This paper presents a secured highly sensitive image encryption system suitable for biomedical applications. The pseudo random number generator of the presented system is based on two discrete logistic maps. The employed maps are: the one dimensional double humped logistic map as well as the two-dimensional delayed logistic map. Different analyses are introduced to measure the performance of the proposed encryption system such as: histogram analysis, correlation coefficients, MAE, NPCR as well as UACI measurements. The encryption system is proven to be highly sensitive to ± 0.001% perturbation of the logistic maps parameters. The system is tested on medical images of palm print as well as Parkinson disease MRI images.

Keywords—Double humped map, Delayed logistic map, bifurcation, encryption, MRI, PRNG, correlation, MAE, NPCR, UACI.

I. INTRODUCTION

Medical imaging technologies have recently been of great importance in diagnosing as well as following the treatment of a lot of diseases. Biomedical images can be generated by many methods, including Computed Tomography (CT), radiography, Magnetic Resonance Imaging (MRI) and more. These images can be digitally archived or transmitted among hospitals or doctors for different clinical purposes. A patient’s medical record is not only text-based personal information, clinical examination or diagnosis, but also it is accompanied by his medical imaging tests. All this information is considered a private matter that shouldn’t be easily accessed. Hence, medical images security has become an important issue for medical services organizations as well as hospitals arousing the need for encrypting these images [1, 2].

Image encryption has become a unique field of research for the past decades. A lot of effort was exerted to modify the traditional image encryption algorithms, specially the use of chaotic systems. Chaotic systems can be either realized in analog or discrete forms [3-7], and one of the most well-known discrete forms is the logistic map [8, 9]. The iterated logistic maps have excelled in many fields like in population biology [10], communication [11]. They are also used in modeling the dynamics of tumor cells [12] and encryption [13]. These maps are the most favorable as key generators in the image encryption field [13-18]. That's because of the special characteristics of these maps like their sensitivity to initial conditions, randomness, unpredictability, ergodicity and parameters control. On the other hand, they are easily reproducible as well as being deterministic. The one dimensional double humped (DH) logistic map is introduced in [19]. The delayed logistic map is a two-dimensional map, which is a delayed version of the conventional logistic map. Time delays offer a better description of real processes. The Neimark-Sacker bifurcation in delayed logistic map was investigated in [20].

The objective of this work is to present an image encryption system, whose PRNG is based on two different chaotic maps, the DH logistic map and the delayed logistic map. The encryption system performance is thoroughly analyzed, through histogram diagrams, as well as other analytical measurements.

II. THE DOUBLE HUMPED/Delayed LOGISTIC MAPS

The double humped (DH) logistic map follows the equation:

\[ x_{n+1} = r(x_n - 1)^2(1 - (x_n - 1)^2), \]  \tag{1}

where \( r \) is the growth rate. The bifurcation diagram of the DH map shown in Fig. 1(a), is very similar to the conventional logistic map bifurcation diagram. The only difference is that here there are repeated bifurcations as \( r \) increases, as well as some gaps in between.

The differential-delay logistic equation with delay \( T \) was introduced long ago in ecological models. A discrete version of this equation was proposed in [20] as:

\[ x_{n+1} = rx_n(1 - x_{n-1}), \]  \tag{2}
where the parameter $r$ is the intrinsic growth rate of the population, and the variables $x_{n+1}$, $x_n$, and $x_{n-1}$ are the population density of generations $n + 1$, $n$ and $n - 1$, respectively. The detailed dynamics analysis of the delayed logistic map is discussed in [15]. The map undergoes complicated variations as $r$ increases. Its bifurcation diagram is shown in Fig. 1(b), where the system turns chaotic at $r=2.27$.

III. IMAGE ENCRYPTION APPLICATION

The block diagram of the proposed encryption system is shown in Fig. 2. The PRNG block, used for key generation, is based on the parameters of the DH map and the delayed logistic map, which are the initial value $x_0$ and the growth rate "$r$". The chosen map is solved recursively to generate the pseudo random numbers $(x)$. For every iteration, a new image pixel and a new value of $x$ are captured. The input pixel is first XORed with the 8 Least Significant Bits (LSBs) of $x$. Then the pixel is again XORed with the output of a delay block of one delay step with zero initial value. In the subsequent iterations, the delay block provides the previously ciphered pixel. The process continues until all pixels are encrypted.

The encryption process was performed on a set of four images, two of which are standard images which are Lena of (128 x 128) pixels and the cameraman image of (256 x 256) pixels. The other two medical images, one is a Parkinson disease MRI image of (300 x 248) pixels which helps in its diagnosis and disease follow up, the other is a Palm Print image with (238 x 211) pixels. The palm print texture structure changes with age and disease. Its shape can be an indicator to kidney deficiency, asthma as well as the diagnosis of some allergic diseases.

IV. ANALYTICAL RESULTS

In this section, different analyses are measured for testing the system performance. Table I shows the encrypted version of the test images using the DH logistic map versus the delayed version of the logistic map. For the 1D-DH map, the initial condition used is $x_0 = 0.1$, and the parameter $r = 8$ to be in the map chaotic region. For the 2D-delayed logistic map, the key is generated using this map, for initial value $x_0 = x_1 = 0.1$ and growth rate $r = 2.27$ to ensure the chaotic region. For each image, a wrong decrypted image is presented as well; this is in response to changing the value of the initial condition value by a +0.001% increase in the decryption process compared to encryption process. From the results shown the image cannot be restored which represents

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Lena</td>
<td><img src="lena_dh.jpg" alt="Image" /></td>
<td><img src="lena_delayed.jpg" alt="Image" /></td>
<td><img src="lena_dh.jpg" alt="Image" /></td>
<td><img src="lena_delayed.jpg" alt="Image" /></td>
</tr>
<tr>
<td>Camran</td>
<td><img src="camran_dh.jpg" alt="Image" /></td>
<td><img src="camran_delayed.jpg" alt="Image" /></td>
<td><img src="camran_dh.jpg" alt="Image" /></td>
<td><img src="camran_delayed.jpg" alt="Image" /></td>
</tr>
<tr>
<td>Palmprint</td>
<td><img src="palmprint_dh.jpg" alt="Image" /></td>
<td><img src="palmprint_delayed.jpg" alt="Image" /></td>
<td><img src="palmprint_dh.jpg" alt="Image" /></td>
<td><img src="palmprint_delayed.jpg" alt="Image" /></td>
</tr>
<tr>
<td>Parkinson</td>
<td><img src="parkinson_dh.jpg" alt="Image" /></td>
<td><img src="parkinson_delayed.jpg" alt="Image" /></td>
<td><img src="parkinson_dh.jpg" alt="Image" /></td>
<td><img src="parkinson_delayed.jpg" alt="Image" /></td>
</tr>
</tbody>
</table>

TABLE I. ENCRYPTED AND WRONG DECRYPTED IMAGES WITH THE DH AND THE DELAYED LOGISTIC MAPS.

A. Histogram Analysis

The histogram shows the distribution of colors inside the image [7]. The strength of any encryption system can be evaluated according to the uniform distribution of the encrypted image histogram so it can effectively prevent the attacks. To evaluate the performance of the encryption system, the histogram distributions of different cipher images using
both proposed maps for key generation are compared in Table II. The histograms show a uniform distribution indicating the strength of the encryption system proposed.

B. Pixel Correlation Analysis

Any normal image pixels are highly correlated to each other. The correlation test is one of the most frequently used methods for testing any encryption system. The correlation coefficient is calculated by

$$ C_{XY} = \frac{\text{cov}(X,Y)}{\sqrt{D_X} \sqrt{D_Y}}, $$

where \( \text{cov}(X,Y) \) calculates the covariance between \( X \) and \( Y \) and \( D_X \) is the variance of \( X \). A decrease in the correlation coefficients of the horizontal, vertical and diagonal pixels of the image is an indication of how strong the encryption system is. It is worth noting that the average correlation coefficients of the encrypted images using both the DH and the delayed maps are in the order of \( 10^{-7} \), illustrated in Table III, which reflects that the pixels are almost uncorrelated in all directions. The horizontal, vertical and diagonal correlation distributions for the original image (Lena) is shown in Fig. 3(a), while the correlation graphs of its encrypted version using the proposed DH map and the delayed logistic map for key generation are shown in Figs. 3(b) and 3(c), respectively.

C. Sensitivity Analysis

Chaotic maps are known for their high sensitivity for any small perturbation in either the initial conditions or the map parameters. In Table IV, it is shown that for a very small perturbation of \( \Delta = \pm 0.001\% \) of the parameter under test whether the initial condition "\( x_0 \)" or the growth rate parameters "\( r \)", the encrypted image cannot be restored to its original image any more. This is due to the high sensitivity for the logistic maps proposed for generating the key. The image under test here is the standard Lena image.

D. Entropy Analysis

Entropy \( H \) is a measure of the image information content, knowing the image probability distribution. For a random variable with a probability distribution \( P_k \), the entropy can be calculated for \( n \) values as follows [18]:

$$ H = -\sum_{k=1}^{n} P_k \log_2(P_k). $$

The entropy is an estimate of image randomness and it is measured in bits. The entropy measurements for different images are shown in Table V for both maps. The entropy values are approximately 8 which validate the encryption system efficiency [7].

E. Differential Attacks

The differential attacks measures are one of the main requirements for secure encryption. They are measured by changing one pixel in the original image and study the effect of this change on the encrypted image, and finding a relation between both images. The absolute change between the encrypted image \( E \) and the source image \( S \) is measured by the mean absolute error (MAE) which is defined as [18]:

-\( \sum_{k=1}^{n} P_k \log_2(P_k). \)
For a normally encrypted image (\(E_2\)), the average light intensity of the differences between two images (\(\text{E}(i,j) - S(i,j)\)) measures the percent change between the two images (\(\text{Change Rate}\)) measures the percent of the number of pixel in the original image. E(i,j) is the pixel value at the location (i,j) where

\[
\text{MAE} = \frac{1}{W \times H} \sum_{l=1}^{H} \sum_{j=1}^{W} |E(i,j) - S(i,j)|, \quad (5)
\]

where W and H are the width and height of the source image (S). For a normally encrypted image (\(E_1\)), and another encrypted image (\(E_2\)) that is encrypted from an image of one pixel change in the original image. E(i,j) is the pixel value at the location (i,j) for the corresponding image E. The NPCR (Number of Pixels Change Rate) measures the percentage of the number of pixel change between the two images (\(E_1\)) and (\(E_2\)), calculated as [18]:

\[
\text{NPCR} = \frac{1}{W \times H} \sum_{i=1}^{H} \sum_{j=1}^{W} D(i,j) \times 100\%, \quad (6a)
\]

\[
D(i,j) = \begin{cases} 
0 & E_1(i,j) = E_2(i,j) \\
1 & E_1(i,j) \neq E_2(i,j)
\end{cases} \quad (6b)
\]

The Unified Average Changing Intensity (UACI) measures the average light intensity of the differences between two images (\(E_1\) & \(E_2\)) [18], and it is calculated as:

\[
\text{UACI} = \frac{1}{W \times H} \sum_{i=1}^{H} \sum_{j=1}^{W} \frac{|E_1(i,j) - E_2(i,j)|}{255} \times 100\%. \quad (7)
\]

Table V shows the results of the differential attacks analysis. MAE, NPCR and UACI for different images using both maps. The MAE results show a great change in the image pixels between the original image and the encrypted one. A major difference in the resulting image due to only a one pixel change is recorded by the NPCR and the UACI numbers are calculated for average of 50 trials.

### V. CONCLUSION

An image encryption system, whose PRNG, based on logistic maps, was presented. The DH logistic map as well as the delayed logistic map were used for key generation. The encryption system was proved to be highly secured through histogram analysis, correlation coefficients, MAE, NPCR and UACI measurements. Standard images as well as medical images of palm print and Parkinson disease MRI images were encrypted using the proposed systems. The system was shown to be highly sensitive to any of the maps parameters with less than a \( \pm 0.001\% \) perturbation.

### REFERENCES


