SECURE IMAGE CRYPTOSYSTEM BASED ON HENON MAP AND ADJUSTED SINE LOGISTIC MAP

HESHAM ALHUMYANI
Department of Computer Engineering, College of Computers and Information Technology, Taif University, Al-Hawiya 21974, KSA
E-mail: h.alhumyani@tu.edu.sa

ABSTRACT
This paper presents a superior confusion-diffusion based color image cryptosystem that is based on employing both the 2D adjusted logistic sine mapping (2D ALSM) and the 2D Henon mapping (2D HM). The encryption phase of the proposed color image encryption scheme utilizes the 2D ALSM in the confusion stage to shuffle the plain color image for m-iterations. The 2D HM is employed in the diffusion stage to diffuse the resulted 2D ALSM based shuffled color image for n-iterations. The decryption phase of the proposed color image encryption scheme follows the same manner of the encryption phase but in a reverse order. The proposed 2D HM-ALSM color image encryption scheme is subjected to a series of security tests to study and investigate its security with respect to several attacks like entropy, histogram, correlation coefficient, differential, occlusion, and noise resistance attacks. The experimental outcomes for the proposed 2D HM-ALSM color image encryption scheme illustrate the superiority and efficiency of the proposed 2D HM-LSM image encryption scheme against different attacks.

Keywords: Henon map, Adjusted Logistic-Sine map, Confusion, Diffusion, Image encryption.

1. INTRODUCTION
Recently, networking and communication technologies have been rapidly developed and become more user-friendly. Technologies such as social network websites and the advancement of smart phones promote and facilitate the sharing of a huge number of digital images between different virtual communities. As matter of fact, there is an urgent need to protect and secure user's private communications from any tampering or unauthorized access and preserve the original data against different attacks. Conventional encryption methods utilized for text like AES, DES, RC5, RC6...etc. [1-3] do not work properly when dealing with images. This is due to the fact that image data contain high levels of correlations and more redundancy which in turn affects the performance in terms of more power to be consumed and more time complexity for processing. To countermeasure these issues, two classes of image encryption have arisen; image data hiding and chaotic image encryption. Image data hiding is defined as the process of embedding and concealing secret data into images where human vision cannot observe and detect [4-8]. However, chaotic image encryption applies non-linear theories using confusion and diffusion according to Shannon [9] that produces random behavior. One of the main advantages of using chaotic based encryption is their sensitivity to the initial conditions and parameters. Chaotic dynamic systems are classified into two main classes: discrete and continuous systems [10-13]. In discrete chaotic systems, chaotic behavior can be obtained in spatial domain by utilizing different chaotic functions applied in an iterative manner. However, continuous systems are employed using differential equations. The chaotic map is defined to be a discrete function which is very sensitive to initial conditions. Chaotic maps can be classified according to its dimension as: a one dimension (1D) like Logistic map, Tent map, and Bernoulli map; a two dimensional (2D) like Baker map, Arnold cat map, Standard map, and Henon map; and a three dimensional (3D) like Logistic map, Tent map, and Bernoulli map [14-17]. Moreover, chaotic based encryption can be applied in both time and frequency domains. Time domain based-encryption schemes employ encryption directly on the image pixel values. Also, selective encryption can be utilized in time domain for achieving efficient time complexity to meet real time applications [18]. On the other hand, image encryption may be employed using different frequency transforms [19-21]. In frequency transform based-encryption, image pixel values are
transformed from time domain into frequency domain using different types of transforms like - Fractional Fourier Transform Domain (FrFT) [19], Discrete Cosine Transform (DCT) [20], and Discrete Wavelet Transform (DWT) [21]. This is done to overcome the issue of statistical characteristics that arises when applying spatial domain-based encryption as well as transform correlated information into different domains which result in additional random behavior and more security. Therefore, chaotic based encryption has been widely used recently in image cryptosystems [22-26].

In [27], a double chaotic image cryptosystem based on tent and logistics maps has been proposed. First, they applied the tent chaotic mapping into the RGB components of the original image. Second, for dual cryptography, they used an additional random image and applied the logistic mapping into its RGB components. Finally, XORing operation is performed between the resulted two images to produce the final cipherimage. In [28], a hybrid cryptosystem based on 1D chaotic map has been proposed. This 1D chaotic map produces a uniform distributed Lyapunov exponent (LE) and ensures preserving the phase space of the original map. They used plainimage pixel values for encryption where the first half of the image pixel values are used to encrypt the second half and vice-versa. In [29], a lightweight digital image cryptosystem that uses chaotic system for wireless network applications has been presented. First, the DCT is utilized to transform image pixels to the frequency domain for the purpose of speeding up the encryption process and remove the statistical similarity between pixels. Second, a 2D Logistics map is used for random confusion of the image pixels along with key generating. Third, for further security, a 2D Henon map is used for diffusing image pixels. Finally, the 2D Logistic map is used again for image substitution.

In [30], an image cryptosystem called 1D sine powered chaotic system is presented. This system depicts the same characteristics of sine map but with two control parameters which results in more chaotic behavior with complex predictability. A secret key is used as an input for the proposed map as an initial value to produce four chaotic-based sequences. The generated sequences are employed for confusion-diffusion at row and column levels. In [31], an optimized 5D image encryption scheme is proposed to solve the hyper-parameter tuning issue for generating secret keys. First, the 5D chaotic map is built using 4D chaotic map with five parameters as the initial state. Second, non-dominated sorting genetic algorithm utilizes a heuristic local search for initial parameters tuning of the 5D chaotic map. Third, the dual-tree complex wavelet transform (DTCWT) is exploited to breakdown the plainimage into several sub-bands. Then, the generated secret key resulted by the optimized 5D map is diffused with the obtained sub-bands. To get the cipherimage, the inverse DTCWT is performed. Finally, since the proposed technique is inefficient in terms of time complexity with large images, parallelism implementation is applied to speed up the execution time of the system.

In [32], a cross chaotic image encryption system based on 2D sine-cosine chaotic map is presented. The secret key is formulated through combining all initial and control parameters together. Then, using 2D sine-cosine chaotic map, two pseudorandom sequences are produced as a function of the obtained secret keys to perform confusion and diffusion respectively on the plainimage. The authors of [33], proposed a lightweight image cryptosystem suitable for real-time applications based on Bulban chaotic map. To increase the sensitivity of the secret key, the mean of all initial parameter values are added to each initial value independently and divided by 2. Also, confusion and diffusion operations are applied on row and column level for an efficient processing performance. In the confusion phase, two sequences are generated using Bülban map to perform circular shift right operation according to the corresponded value of the sequence where one sequence is to identify the number of shifts for rows and the other sequence is assigned to deal with columns. In the diffusion phase, two random rows are generated and placed at the top and the bottom of the shuffled matrix. Finally, four sequences are generated using Bülban map to perform a bitwise-XORing operation and then produce the final cipherimage.

Henon chaotic map is introduced by [34] as simplification model of Lorenz model [35], which represents 2D dynamic system with quadratic non-linear characteristics and has been practically utilized recently in the literature [36-38]. Another class of hybrid chaotic mapping called Logistic Adjusted Sine Map is proposed by [39] to utilize characteristics of both sine map and logistic map to provide more chaotic random behavior as well as additional security. In this paper, we present a hybrid confusion-diffusion image cryptosystem based on using the 2D Henon mapping (2D HM) and the 2D adjusted logistic sine mapping (2D ALSM). We aim to apply both encryption/decryption procedures in
order to investigate the performance of the proposed 2D HM-ALSM image encryption scheme with respect to different security metrics like statistical, sensitivity and differential tests.

The paper rest is sectioned as follows: Section 2 presents the employed tools in the proposed encryption scheme which involve the 2D HM and the 2D ALSM. Section 3 shows the encryption/decryption procedures of the proposed 2D HM-ALSM image encryption scheme. Section 4 explores and discusses the experimental results of the proposed 2D HM-ALSM image encryption scheme. Finally, Section 5 presents the conclusions of the paper.

2. PRELIMINARIES

In this section, we present and overview the employed tools in the proposed 2D HM-ALSM image encryption scheme. These tools include both the 2D ALSM and the 2D HM.

2.1 The 2D ALSM

The 2D ALSM is a hybrid nonlinear dynamic chaotic mapping approach that is composed of both logistic map [40] and sine map [41]. This hybrid 2D ALSM can overcome the drawbacks of using either logistic map or sine map independently due to their simple behavior, and small key space. Therefore, coupling both the logistic and the Sine maps result in a complex chaotic behavior. In this hybrid technique, the logistic map is employed first for confusion/diffusion and then the output is set to be the input for the sine map for adjustment. Then the plane is extended from one dimension into two dimensions. The mathematical formula of the 2D ALSM can be defined as [39]:

\[
\begin{align*}
A_{i+1} &= \lambda \left( 4B_i A_i (1 - A_i) + (1 - \lambda) \sin(\pi B_i) \right) \\
B_{i+1} &= \lambda \left( 4A_i B_i (1 - B_i) + (1 - \lambda) \sin(\pi A_i) \right)
\end{align*}
\]

where \(\lambda \in [0,1]\) represents the control parameter.

2.2 The 2D HM

The 2D HM is one form of 2D dynamic chaotic system that exhibits a scrambling-based confusion behavior. It works through changing the image pixels positions. The 2D HM is mathematically defined as [42]:

\[
\begin{align*}
A_i &= 1 - \alpha A_i + B_i \\
B_i &= \beta B_i
\end{align*}
\]

where \(\alpha\) and \(\beta\) are the control parameters, \(A\) and \(B\) represent iteration values, and \(k\) manifest the iterations number.

3. THE PROPOSED HM-ALSM IMAGE CRYPTOSYSTEM

In this section, the enciphering and the deciphering processes of the proposed 2D HM-ALSM are presented. As mentioned in section 2, both 2D HM and ALSM have been used to build the proposed HM-ALSM image cryptosystem.

3.1 Encryption Procedure

The enciphering algorithm of the proposed 2D HM-ALSM is depicted in Fig. 1. The procedure of the proposed cryptosystem is outlined as follows:

1. Read an input plainimage.
2. Split the plainimage into its RGB components.
3. Each of RGB color channels of the plainimage is taken respectively according to step 2.
4. Confusion operation is applied using the 2D ALSM on the plainimage for \(n\)-rounds.
5. The output scrambled image is used in diffusion operation using the 2D HM for \(m\)-rounds.
6. Repeat step 4 and 5 for each of RGB channels.
7. Finally, the cipherimage is produced by merging the RGB obtained cipher image channels and transmitted by communication channels.

3.2 Decryption Procedure

The deciphering procedure includes inverse operations of the ciphering algorithm. The procedure of the proposed 2D HM-ALSM image cryptosystem can be outlined as follows:

1. Receive the RGB color cipherimage.
2. Split the RGB color cipherimage into its RGB components.
3. Each of RGB color channel of the cipherimage is taken respectively according to step 2.
4. The diffusion operation is applied using the inverse of 2D HM for \(m\)-rounds.
5. The output of the inverse diffusion operation is subjected to a confusion using the inverse of 2D ALSM for \(n\)-rounds.
6. Repeat step 4 and 5 for each of the RGB color channels.
7. Finally, the plainimage is reconstructed by merging the RGB components.
4. EXPERIMENTAL TESTS AND DISCUSSIONS

This section is dedicated to examine and test the security of the proposed 2D HM-ALSM image encryption scheme. This is done through conducting a set of security tests. In addition, the proposed 2D HM-ALSM image encryption scheme is compared to both 2D HM and 2D ALSM in terms of several security measurements including the most encryption metrics statistical, entropy and differential examination, visual notification, and noise tests. The test experiments are employed using three 512×512 color images as plainimages. These color plainimages include Lena, Peppers, and Baboon as depicted in Fig. 2.

4.1 Visual Notification

The visually notified outcomes of encrypted color Lena, Peppers, and Baboon with the proposed 2D HM-ALSM image encryption scheme, 2D HM, and 2D ALSM image cryptosystems are shown in Fig. 3, Fig. 4, and Fig. 5 respectively. It is obvious that the resulted cipherimages are totally distinct from their respected plainimages. In addition, the visually notified encrypted color Lena, Peppers, and Baboon ensure the efficiency of the proposed 2D HM-ALSM image encryption scheme in concealing all the details of the corresponding original color images.
4.2 Histogram Testing

To achieve an efficient cipherimage, the cipherimage histogram must be uniformly distributed and completely different from its corresponding plainimage. The histograms of the tested color Lena, Peppers, and Baboon cipherimages are illustrated in Figs. 6-8. The histogram outcomes for the 2D ALSM encryption scheme indicate that the histogram results for both plainimages and their respected cipherimages are identical. This is due to the fact that the 2D ALSM is just perform scrambling and so does not change the histogram. However, the histogram outcomes of the proposed 2D HM-ALSM and 2D HM encryption schemes indicate that the histogram results for both plainimages and their respected cipherimages are completely different.

\begin{equation}
\text{Ent}(x) = -\sum_{i} P(x_i) \log_2 P(x_i)
\end{equation}

where \( \text{Ent}(x) \) defines the entropy value in bits. \( P(x) \) is the probability of occurrence of \( x \). Table 1 lists the entropy values for both RGB plainimages and their corresponding cipherimages using 2D ALSM, 2D HM and the proposed 2D HM-ALSM encryption schemes for color Lena, Peppers, and Baboon images. The entropy outcomes shown in Table 1 ensure and confirm the
efficiency of the proposed 2D HM-ALSM encryption scheme whose entropy values are near to its optimal value of 8.

4.4 Differential Analysis

The differential analysis is employed using both number of pixel change rate (NPCR) and unified average changing intensity (UACI) metrics to estimate the impact of changing just only one pixel in two identical plainimages on their corresponding encrypted images. The NPCR metric can be expressed as [43]:

\[ \text{NPCR}_{R,G,B}(x^I, x^E) = \frac{\sum |x^I_r - x^E_r|^2}{N^2} \times 100\% \]  

(4)

where \( N \) is total image pixels number and \( x^I_r, x^E_r \) is measured using Eq. 5 as:

\[ x^I_r = \begin{cases} 1, & \text{if } R^I_r = R^E_r \text{ or } G^I_r = G^E_r \text{ or } B^I_r = B^E_r \\ 0, & \text{otherwise} \end{cases} \]

(5)

where \( R^I_r, G^I_r, B^I_r \) and \( R^E_r, G^E_r, B^E_r \) are the RGB components of the two color encrypted images \( I^E, E^E \).

The UACI\(_{R,G,B}\) metric can be expressed as [43]:

\[ \text{UACI}_{R,G,B}(x^I, x^E) = \frac{1}{N^2} \sum_{i=1}^{N} \left( \frac{|\text{hist}(i) - \text{hist}(i)|}{\text{AVG}} \right) \times 100\% \]  

(6)

Table 2 lists the NPCR and UACI outcomes using 2D ALSM, 2D HM and the proposed 2D HM-ALSM encryption schemes for RGB color Lena, Peppers, and Baboon images. The NPCR and UACI outcomes reflect the high sensibility of the proposed 2D HM-ALSM encryption scheme regarding tiny modifications such as one-pixel change.

4.5 Ciphering Quality Assessment

One of the major image cryptosystem assessment tools is to investigate the quality of encryption in terms of different metrics like correlation coefficient (\( r_{xy} \)), histogram deviation (\( D_h \)), and irregular deviation (\( D_i \)). Therefore, correlation coefficient, histogram deviation, and irregular deviation tests are applied to evaluate the proposed 2D HM-ALSM encryption schemes for RGB color Lena, Peppers, and Baboon images. With respect to correlation coefficients, an efficient and secure encryption scheme must obtain high values. With respect to irregular deviation, it must be low for an efficient image cryptosystem.

The mathematical formulations of \( r_{xy}, D_h, \) and \( D_i \) are shown as follows [44]:

\[ r_{xy} = \frac{E[I]E[PI] - E[I]E[PI]}{\sqrt{E[I^2] - E[I]^2} \sqrt{E[PI^2] - E[PI]^2}} \]

(7)

\[ D_h = \frac{|\text{hist}(i) - \text{hist}(i)|}{\text{AVG}} \]

(8)

\[ D_i = \frac{\sum |E[I_r] - E[PI_r]|}{\text{Max}} \]

(9)

where \( EI, \) and \( PI \) are the encrypted image and plainimage. The \( \text{diff}(i) \) represents the absolute deviation between the plainimage and the encrypted images at intensity \( i \). The \( \text{hist}(i) \) is the encrypted image histogram at intensity \( i \). \( AVG \) is the histogram distribution of an ideal encrypted. \( M, N \) are the dimension of both the plainimage and the encrypted images. The obtained encryption quality results of the 2D ALSM, 2D HM and the proposed 2D HM-ALSM encryption schemes for RGB color Lena, Peppers, and Baboon images are presented in Table 3. The achieved results of the proposed 2D HM-ALSM encryption scheme validate the superiority of the proposed 2D HM-ALSM encryption scheme compared to both 2D ALSM and 2D HM.

4.6 Noise Immunity Analysis

The noise immunity analysis is employed to examine and investigate the resistance of the proposed 2D HM-ALSM image encryption scheme against different types of noise. The different types of used noises involve the additive white Gaussian noise (AWGN), Salt and peppers noise, and speckle noise. The noise immunity test is employed with the following scenario. The tested plainimage is firstly encrypted using the proposed 2D HM-ALSM image ciphering technique and the noise is added to the cipherimage. After that, the noisy cipherimage is decrypted, and the decrypted image is observed visually and mathematically analyzed with different measures like the PSNR, SSIM, and FSIM.
defines the spatial domain of the image and the resulted deciphered image.

The structural similarity (SSIM) metric is employed to estimate the percentage of similarity among the original color image and the resulted deciphered image to evaluate efficiency of the proposed 2D HM-ALSM image encryption scheme against different types of noise. The SSIM values are expressed in the interval range from 0 to 1, such that 1 indicates two fully similar images. The SSIM values are adequate and reasonable as the variance increased. However, the obtained SSIM and FSIM values decreased against different types of noise are given in in Tables 5-6.

Regarding SSIM and FSIM, it is required to achieve high values of SSIM and FSIM to confirm efficient noise resistance. The SSIM and FSIM among the original color image and the resulted deciphered image are estimated to evaluate efficiency of the proposed 2D HM-ALSM image encryption scheme against different types of noise. The estimated SSIM and FSIM values of the proposed 2D HM-ALSM image encryption scheme against different types of noise are given in in Tables 5-6.

For different types of noises, it is observed that the obtained SSIM and FSIM values decreased as the variance increased. However, the obtained SSIM and FSIM values are adequate and reasonable with distinct noise variances. Thence, the SSIM and FSIM values are expressed in the interval range from 0 to 1, such that 1 indicates two fully similar images. The FSIM can be defined as [45]:

\[
FSIM_{x,y}(I) = \frac{\sum_{x,y} (T(x,y) - \overline{T})^2}{\sum_{x,y} (T(x,y) - \overline{I})^2}
\]

where \(T(x,y)\) represents the estimated similarity among the original color image and the resulted deciphered image, \(\overline{T}\) defines the spatial domain of the image, and the \(\overline{I}\) represents the estimated value of the phase congruency.

The results of the noise resistance evaluation for decrypted color Lena, Peppers, and Baboon images with AWGN, Salt and Peppers noise, and speckle noise at different variances ranged from 0.05 to 0.20 with step of 0.05 are given in Table 4 and Figs. 9-11. The noise immunity results as shown in Table 4 and Figs. 9-11 confirmed the efficiency and the ability of the proposed 2D HM-ALSM image cryptosystem in withstanding the AWGN using variable variances.

Table 3. The encryption quality results of RGB plain/cipher images using 2D ALSM, 2D HM and the proposed 2D HM-ALSM encryption schemes for color Lena, Peppers, and Baboon images.
FSIM results assure the superiority of the 2D HM-ALSM image cryptosystem in the presence of AWGN, Salt & peppers noise, and Speckle noise.

Table 4. PSNR values of the deciphered Red, Green and Blue components using the proposed 2D HM-ALSM image cryptosystem in the presence of AWGN, Salt & peppers noise, Speckle noise for color Lena, Peppers, and Baboon images.

<table>
<thead>
<tr>
<th>Image</th>
<th>AWGN</th>
<th>Salt &amp; peppers noise</th>
<th>Speckle noise</th>
</tr>
</thead>
</table>

Table 5. SSIM values of the deciphered Red, Green and Blue components using the proposed 2D HM-ALSM image encryption scheme in the presence of AWGN, Salt & peppers noise, Speckle noise for color Lena, Peppers, and Baboon images.

<table>
<thead>
<tr>
<th>Image</th>
<th>SSIM</th>
<th>AWGN</th>
<th>Salt &amp; peppers</th>
<th>Speckle</th>
</tr>
</thead>
<tbody>
<tr>
<td>R</td>
<td>0.0030 0.0030 0.0029 0.0028</td>
<td>0.0031 0.0030 0.0030 0.0029</td>
<td>0.0030 0.0030 0.0029 0.0029</td>
<td></td>
</tr>
<tr>
<td>G</td>
<td>0.3825 0.2979 0.2306 0.1945</td>
<td>0.6018 0.4495 0.3600 0.2984</td>
<td>0.7210 0.6202 0.5565 0.5105</td>
<td></td>
</tr>
<tr>
<td>B</td>
<td>0.3275 0.2227 0.1791 0.1518</td>
<td>0.5708 0.4127 0.3183 0.2625</td>
<td>0.6810 0.5458 0.4619 0.4057</td>
<td></td>
</tr>
</tbody>
</table>

Table 6. FSIM values of the deciphered Red, Green and Blue components using the proposed 2D HM-ALSM image encryption scheme in the presence of AWGN, Salt & peppers noise, Speckle noise for color Lena, Peppers, and Baboon images.

<table>
<thead>
<tr>
<th>Image</th>
<th>FSIM</th>
<th>AWGN</th>
<th>Salt &amp; peppers</th>
<th>Speckle</th>
</tr>
</thead>
<tbody>
<tr>
<td>R</td>
<td>0.4329 0.4227 0.4180 0.4156</td>
<td>0.4447 0.4362 0.4298 0.4255</td>
<td>0.4393 0.4299 0.4244 0.4208</td>
<td></td>
</tr>
<tr>
<td>G</td>
<td>0.7079 0.6284 0.5889 0.5586</td>
<td>0.8437 0.7546 0.6861 0.6441</td>
<td>0.8744 0.8231 0.7900 0.7616</td>
<td></td>
</tr>
<tr>
<td>B</td>
<td>0.6494 0.5699 0.5287 0.5046</td>
<td>0.8222 0.7266 0.6585 0.6139</td>
<td>0.8538 0.7864 0.7367 0.7048</td>
<td></td>
</tr>
</tbody>
</table>

ISSN: 1992-8645  www.jatit.org  E-ISSN: 1817-3195
<table>
<thead>
<tr>
<th>Image</th>
<th>Color channel</th>
<th>AWGN Noise</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>0.05</td>
</tr>
<tr>
<td>Lena</td>
<td>R</td>
<td><img src="image1.png" alt="Image" /></td>
</tr>
<tr>
<td></td>
<td>G</td>
<td><img src="image5.png" alt="Image" /></td>
</tr>
<tr>
<td></td>
<td>B</td>
<td><img src="image9.png" alt="Image" /></td>
</tr>
<tr>
<td>Baboon</td>
<td>R</td>
<td><img src="image13.png" alt="Image" /></td>
</tr>
<tr>
<td></td>
<td>G</td>
<td><img src="image17.png" alt="Image" /></td>
</tr>
<tr>
<td></td>
<td>B</td>
<td><img src="image21.png" alt="Image" /></td>
</tr>
<tr>
<td></td>
<td>RGB</td>
<td><img src="image25.png" alt="Image" /></td>
</tr>
</tbody>
</table>

Fig. 9. The resulted deciphered Red, Green and Blue components using the proposed 2D HM-ALSM image encryption scheme in the existence of AWGN noise for color Lena, Peppers, and Baboon images.
<table>
<thead>
<tr>
<th>Image</th>
<th>Color channel</th>
<th>Salt &amp; Peppers Noise</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>0.05</td>
</tr>
<tr>
<td>Lena</td>
<td>R</td>
<td><img src="image1.png" alt="Image" /></td>
</tr>
<tr>
<td>Lena</td>
<td>G</td>
<td><img src="image5.png" alt="Image" /></td>
</tr>
<tr>
<td>Lena</td>
<td>B</td>
<td><img src="image9.png" alt="Image" /></td>
</tr>
<tr>
<td>Lena</td>
<td>RGB</td>
<td><img src="image13.png" alt="Image" /></td>
</tr>
<tr>
<td>Peppers</td>
<td>R</td>
<td><img src="image17.png" alt="Image" /></td>
</tr>
<tr>
<td>Peppers</td>
<td>G</td>
<td><img src="image21.png" alt="Image" /></td>
</tr>
<tr>
<td>Peppers</td>
<td>B</td>
<td><img src="image25.png" alt="Image" /></td>
</tr>
<tr>
<td>Peppers</td>
<td>RGB</td>
<td><img src="image29.png" alt="Image" /></td>
</tr>
<tr>
<td>Baboon</td>
<td>R</td>
<td><img src="image33.png" alt="Image" /></td>
</tr>
<tr>
<td>Baboon</td>
<td>G</td>
<td><img src="image37.png" alt="Image" /></td>
</tr>
<tr>
<td>Baboon</td>
<td>B</td>
<td><img src="image41.png" alt="Image" /></td>
</tr>
<tr>
<td>Baboon</td>
<td>RGB</td>
<td><img src="image45.png" alt="Image" /></td>
</tr>
</tbody>
</table>

**Fig. 10.** The resulted deciphered Red, Green and Blue components using the proposed 2D HM-ALSM image encryption scheme in the existence of Salt & peppers noise for color Lena, Peppers, and Baboon images.
<table>
<thead>
<tr>
<th>Image</th>
<th>Color channel</th>
<th>Speckle Noise</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>0.05</td>
</tr>
<tr>
<td>Lena</td>
<td>R</td>
<td>![Image]</td>
</tr>
<tr>
<td></td>
<td>G</td>
<td>![Image]</td>
</tr>
<tr>
<td></td>
<td>B</td>
<td>![Image]</td>
</tr>
<tr>
<td></td>
<td>RGB</td>
<td>![Image]</td>
</tr>
<tr>
<td>Peppers</td>
<td>R</td>
<td>![Image]</td>
</tr>
<tr>
<td></td>
<td>G</td>
<td>![Image]</td>
</tr>
<tr>
<td></td>
<td>B</td>
<td>![Image]</td>
</tr>
<tr>
<td></td>
<td>RGB</td>
<td>![Image]</td>
</tr>
<tr>
<td>Baboon</td>
<td>R</td>
<td>![Image]</td>
</tr>
<tr>
<td></td>
<td>G</td>
<td>![Image]</td>
</tr>
<tr>
<td></td>
<td>B</td>
<td>![Image]</td>
</tr>
<tr>
<td></td>
<td>RGB</td>
<td>![Image]</td>
</tr>
</tbody>
</table>

Fig. 11. The resulted deciphered Red, Green and Blue components using the proposed 2D HM-ALSM image encryption scheme in the existence of Speckle noise for color Lena, Peppers, and Baboon images.
5. CONCLUSION
The paper presents an efficient confusion-diffusion image cryptosystem scheme based on 2D ALSM and 2D HM. In the proposed encryption system, confusion and diffusion operations have been utilized to provide more random behavior. This is realized through 2D ALSM for confusion stage and 2D HM for diffusion stage. These two employed mechanisms have ensured the capability of obtaining an efficient 2D HM-ALSM image encryption system. The proposed 2D HM-ALSM image encryption scheme is examined using multiple security metrics such as statistical, entropy, differential examination, visual notification, and noise resistance tests. Simulation results have validated the performance superiority of the proposed 2D HM-ALSM image encryption scheme.

REFERENCES:


