Performance analysis of transformation and bogdonov chaotic substitution based image cryptosystem

Prajwalasimha S. N., Basavaraj L.
Department of Electronics and Communication Engineering, ATME Research Centre, India

ABSTRACT

In this article, a combined Pseudo Hadamard transformation and modified Bogdonov chaotic generator based image encryption technique is proposed. Pixel position transformation is performed using Pseudo Hadamard transformation and pixel value variation is made using Bogdonov chaotic substitution. Bogdonov chaotic generator produces random sequences and it is observed that very less correlation between the adjacent elements in the sequence. The cipher image obtained from the transformation stage is subjected for substitution using Bogdonov chaotic sequence to break correlation between adjacent pixels. The cipher image is subjected for various security tests under noisy conditions and very high degree of similarity is observed after deciphering process between original and decrypted images.

Keywords: Chaotic generator, Confidentiality, Correlation, Encryption, Substitution

Copyright © 2020 Institute of Advanced Engineering and Science. All rights reserved.

1. INTRODUCTION

Images are pictorial depiction of information. Due to swift maturation in internet technology, digital images being major class of multimedia, plays a vital role in communication systems. These images are characterized inimitably by high inter pixel redundancy, strong correlation between adjacent pixels and bulk data capacity [1-7]. Confidentiality is one of the dominant facets of communication system. Fortification of information can be accomplished by adopting an efficient cryptosystem, which should encrypt and decrypt the information without flaws. More prevalently and habitually used encryption algorithms such as Rivest, Shamir and Adleman (RSA), Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA) and Advance Encryption Standards (AES) are inapposite for images due to their inimitable characteristics [2]. Chaotic systems found proliferate implementation in the fields of cryptography, due to their intrinsic properties such as volatility, subtlety to the initial conditions, similar casualness and aperiodicity [3, 8]. With the help of chaotic theory, the inter pixel redundancy and strong correlation between adjacent pixels can be effectively reduced.

In many low dimensional chaos based cryptographic algorithms, the cipher data directly depends on chaotic orbit of a single chaotic system. Due to this, many low dimensional chaotic systems are more prone to phase space reconstruction attacks [9]. Such kind of attacks can be reduced by using S-box (Substitution box) in the algorithm. Complexity of cryptanalysis and brute force attacks can be further reduced by increasing the size of S-box in the algorithm. One such technique is developed by Silva-García and et al [10]. They introduced S-boxes in Advanced Encryption Standard (AES) algorithm to increase the level of security. Nonlinear chaotic differential equations are used to generate random numbers inside the S-box. But immunity against noise has not been noticed in the algorithm.

A double humped logistic map has been developed by Lingfeng & et al. [11] by introducing general parameters to the existing chaotic map to generate pseudo random key sequence for the substitution stage. Robustness of the algorithm against Gaussian noise has been noticed but not against other kind of noises. Better UACI values are observed for various images but considerable differences in the NPCR values are noticed compared to ideal values. Rasul Enayatifar & et al. [12] developed combined permutation and diffusion technique using 3-D logistic chaotic map. Better entropy is observed in the absence of noise for many standard images but considerable difference in the values of NPCR and UACI is observed compared to ideal values. A combined 1-D logistic map and 2-D Baker chaotic map based block wise permutation algorithm has been developed by Lingfeng Liu & et al. [13]. Even though low dimensional chaotic maps are considered, phase space is made large by multiple chaotic maps. Very minimum correlation between the adjacent pixels in the cipher image has been noticed along with slightly high entropy but considerable difference in the values of NPCR and UACI is observed compared to ideal values for few standard images.

Based on the above considerations a combined 2-D Pseudo Hadamard chaotic transformation (MPHT) and 2-D Bogdonov chaotic random diffusion based algorithm has been proposed in which a large phase space is considered along with a substitution image. The paper is organized as follows: Section 2 describes the proposed scheme. Section 3 with statistical and differential analysis followed by conclusion in Section 4.

2. RESEARCH METHOD

Three stages per round are involved in the encryption process: Transformation, Diffusion and Substitution. Modified Pseudo Hadamard transformation is used in the first stage and random sequence generated by Bagdonov chaotic generator is used in the substitution stage. Figure 1 illustartes the flow diagram of the system.

2.1. Encryption algorithm

Step1: Original image of size $2^n \times 2^n$ is transformed using modified Pseudo Hadamard transformation.

$$H1'(x, y) = H((a + b + c) \mod 2^n, (a + 2b + c) \mod 2^n) \quad 1 < a, b < 2^n$$ (1)

Where,

$H(a, b)$ is the host image of size $2^n \times 2^n$

$H1'(x, y)$ is the transformed image of size $2^n \times 2^n$

$c$ is the constant ($c = 37$)

Step2: Block truncated substitution image of size $2^n \times 2^n$ is transformed using modified Pseudo Hadamard transformation.

$$S1'(x, y) = S^{t}((a' + b' + c) \mod 2^n, (a' + 2b' + c) \mod 2^n) \quad 1 < a', b' < 2^n$$ (2)

Where,

$S1'(a', b')$ is the block truncated substitution image of size $2^n \times 2^n$

$S^{t}(x, y)$ is the transformed truncated image of size $2^n \times 2^n$

$c$ is the constant ($c = 37$)

Step3: Both transformed images are subjected for bitwise XOR operation

$$C1(x, y) = H'(x, y) \oplus S'(x, y)$$ (3)

Step4: The cipher image from first stage is subjected for substitution with pre-defined S-box.

$$C2(x, y) = C1(x, y) \oplus S-box$$ (4)

Step4: The cipher image from substitution stage is subjected for diffusion with random sequence generated Bogdonov chaotic equation.

$$x' = (x + y') \mod 2^n$$ (5)

$$y' = (y + \epsilon y' + Kx'(x' - 1) + \mu x'y') \mod 2^n$$ (6)
Where,

\[
\begin{align*}
\epsilon &= 7(d)^2 \\
K &= 9(d)^2 \\
\mu &= 3(d) \\
d &= \sum_{i=1}^{256} \sum_{j=1}^{256} H(a, b)
\end{align*}
\]

\[
C3(x, y) = C2(x, y) \oplus x'
\]  (7)

Where,

\[
C3(x, y)
\]

is the cipher image after diffusion of size \(2^n \times 2^n\)

Step5: The number of execution rounds \((d)\) is placed in the four extreme corners of the cipher image along with the respective pixel values.

2.2. Decryption algorithm

The number of rounds for decryption stage \((d)\) is taken from the pixel values in the four extreme corners of the cipher image.

Step1: The cipher image is then subjected for XOR operation with random sequence generated Bogdonav chaotic equation with the same constant co-efficient.

\[
x' = (x + y') \mod 2^n
\]  (8)

\[
y' = (y + \epsilon y' + Kx'(x' - 1) + \mu x'y') \mod 2^n
\]  (9)

Where,

\[
\begin{align*}
\epsilon &= 7(d)^2 \\
K &= 9(d)^2 \\
\mu &= 3(d)
\end{align*}
\]
\[ C2'(x, y) = C3'(x, y) \oplus x' \]  

(10)

Step 2: The obtained cipher image XORed with the elements of S-box used for encryption.

\[ C1'(x, y) = C3'(x, y) \oplus S-box \]  

(11)

Step 3: The block truncated substitution image is subjected for MPHT with same constant and then XORed with cipher image from previous stage.

\[ S1'(x, y) = S^t(a' + b' + c) \mod 2^n, (a' + 2b' + c) \mod 2^n \]  

(12)

\[ H1'(x, y) = C1'(x, y) \oplus S'(x, y) \]  

(13)

Step 4: The obtained image from previous step is subjected for inverse MPHT to get original image.

\[ H'(a, b) = H1'(5x - 4y - c) \mod 2^n, (y - x) \mod 2^n \]  

(14)

3. EXPERIMENTAL RESULTS

Standard test images are considered from Computer Vision Group (CVG), Dept. of Computer Science and Artificial Intelligence, University of Granada, Spain. Matlab software is used for performance analysis and implementation. Performance analysis is made based on various security tests. Table 1 compares resultant Entropy, Correlation, UACI and NPCR of different encryption schemes with the proposed system. The results indicate very less correlation between the adjacent pixels after substitution phase along with high entropy value indicating that the pixel values are altered effectively in the cipher image.

<table>
<thead>
<tr>
<th>Images</th>
<th>Entropy</th>
<th>Correlation</th>
<th>UACI = 33.4635% [14]</th>
<th>NPCR = 99.6093% [14]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peppers</td>
<td>7.9954</td>
<td>-0.0040</td>
<td>33.3761</td>
<td>99.6490</td>
</tr>
<tr>
<td>Cameraman</td>
<td>7.9972</td>
<td>0.0040</td>
<td>33.2971</td>
<td>99.6231</td>
</tr>
<tr>
<td>Barche</td>
<td>7.9973</td>
<td>-0.0041</td>
<td>33.3763</td>
<td>99.6201</td>
</tr>
<tr>
<td>Carnev</td>
<td>7.9971</td>
<td>-9.7275e-04</td>
<td>33.3590</td>
<td>99.5651</td>
</tr>
<tr>
<td>Donna</td>
<td>7.9973</td>
<td>1.6005e-04</td>
<td>33.4637</td>
<td>99.6460</td>
</tr>
<tr>
<td>Foto</td>
<td>7.9968</td>
<td>-0.0028</td>
<td>33.4974</td>
<td>99.5667</td>
</tr>
<tr>
<td>Galaxia</td>
<td>7.9972</td>
<td>0.0024</td>
<td>33.4866</td>
<td>99.5773</td>
</tr>
<tr>
<td>Leopard</td>
<td>7.9972</td>
<td>0.0013</td>
<td>33.3751</td>
<td>99.3911</td>
</tr>
<tr>
<td>Montage</td>
<td>7.9966</td>
<td>-0.0050</td>
<td>33.3403</td>
<td>99.6384</td>
</tr>
<tr>
<td>Clock</td>
<td>7.9969</td>
<td>0.0038</td>
<td>33.3330</td>
<td>99.6094</td>
</tr>
<tr>
<td>Vacas</td>
<td>7.9974</td>
<td>-4.2689e-04</td>
<td>33.3868</td>
<td>99.6140</td>
</tr>
<tr>
<td>Fiore</td>
<td>7.9972</td>
<td>0.0058</td>
<td>33.4856</td>
<td>99.6262</td>
</tr>
<tr>
<td>Mapasp</td>
<td>7.9972</td>
<td>0.0040</td>
<td>33.2827</td>
<td>99.6201</td>
</tr>
<tr>
<td>Soil</td>
<td>7.9970</td>
<td>0.0026</td>
<td>33.3852</td>
<td>99.6017</td>
</tr>
<tr>
<td>Mesa</td>
<td>7.9976</td>
<td>0.0077</td>
<td>33.3114</td>
<td>99.6155</td>
</tr>
<tr>
<td>Papav</td>
<td>7.9969</td>
<td>4.2616e-04</td>
<td>33.4553</td>
<td>99.6216</td>
</tr>
<tr>
<td>Tulips</td>
<td>7.9974</td>
<td>0.0058</td>
<td>33.4337</td>
<td>99.5987</td>
</tr>
</tbody>
</table>

Performance analysis of transformation and bogdonov chaotic substitution based ... (Prajwalasimha S N)
3.1. Noise interference

The correlation coefficient decides the similarity between retrieved (decrypted) and original images [24]. The performance analysis of decrypted image under noisy condition is decided by comparing the correlation coefficient between decrypted and original images. Figure 2 illustrates retrieved and original image under different noisy conditions and Table 2 describes the similarity in the order of correlation between the decrypted and original images under noise interference. If the correlation coefficient is equal to unity, the retrieved image is same as that of the original watermark. The cipher image is considered under various noisy conditions and the performance analysis of the algorithm is made after decrypting the noisy cipher image.

Figure 2. Performance analysis of retrieved and original image under noisy conditions

Table 2. Performance analysis of retrieved and original image under noisy attacks

<table>
<thead>
<tr>
<th>Noise Interference</th>
<th>Correlation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pepper &amp; Salt</td>
<td>0.8617</td>
</tr>
<tr>
<td>Gaussian</td>
<td>0.7062</td>
</tr>
<tr>
<td>Poisson</td>
<td>0.8449</td>
</tr>
<tr>
<td>Speckle</td>
<td>0.6527</td>
</tr>
<tr>
<td>LSB neutralization attack</td>
<td>0.9790</td>
</tr>
</tbody>
</table>

3.2. Inference

The correlation co-efficient value drops to a minimum 0.6527 with speckle (multiplicative) noise in cipher image indicating 65% similarity between the corresponding pixels in original and retrieved images. Due to LSB neutralization attack, the correlation co-efficient of 0.9790 is observed indicating 98% similarity between original and retrieved images. It has been observed that, an average of 81% similarity between original and retrieved images is observed under noisy conditions. And hence the proposed algorithm gives better results under noise attacks. Figure 3 illustrates similarity in the order of correlation between
the de-crypted and original images under different noise densities. Figure 4 Illustration of resultant images under different stage of the crypto-process. Also very close to the ideal values of Unified Average Changing Intensity (UACI=33.39%) but slight less and Number of Pixel Changing Rate (NPCR=99.61%) equal to the ideal value, slightly greater than that as observed in non-Chaotic substitution [25] are noticed from the outcome of the standard images.

![Correlation between the retrieved and original watermarks under noise interference](image)

**Figure 3.** Correlation between the retrieved and original watermarks under noise interference

<table>
<thead>
<tr>
<th>Host image (Lena)</th>
<th>Substitution image (Concordaerial)</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="MPHT transformed image (Lena)" /></td>
<td><img src="image" alt="Truncated &amp; MPHT transformed image (Concordaerial)" /></td>
</tr>
<tr>
<td><img src="image" alt="Cipher image of final stage (Lena)" /></td>
<td><img src="image" alt="De-Crypted image of Lena" /></td>
</tr>
</tbody>
</table>

**Figure 4.** Illustration of Host image, Substitution image and Cipher image after transformation, diffusion and substitution stages

*Performance analysis of transformation and bogdonov chaotic substitution based ... (Prajwalasimha S N)*
4. CONCLUSION
In the proposed encryption scheme, Pseudo Hadamard transformation is used in the transformation stage to vary pixel positions and Bogdonov chaotic random sequence generator is used in the substitution stage to vary the pixel values in an image. High redundancy and strong correlation between the adjacent pixels are effectively reduced by the proposed technique. High degree of randomness obtained from Bogdonov chaotic generator in the substitution stage leads to achieve better entropy in the cipher image. Correlation between host and cipher images is very less indicating poor similarities between them. Average values of 99.61% number of pixel changing rate (NPCR) is observed which is almost equal to the ideal value and an average value of 33.39% unified average changing intensity (UACI) is obtained which is very close to the ideal values, for a set of twenty standard images. Further, more number of chaotic generators can be used to get random sequences for substitution stage of encryption to increase the level of security.

REFERENCES
Performance analysis of transformation and bogdonov chaotic substitution based … (Prajwalasimha S N)

BIOGRAPHIES OF AUTHORS

Prajwalasimha S N received Bachelor of Engineering (B.E) Degree in Electronics & Communication from Visvesvaraya Technological University, India in 2012, Master of Technology (M.Tech) Degree in Digital Electronics & Communication Systems from Visvesvaraya Technological University, India in 2014 and pursuing Doctoral Degree (Ph.D) in the field of Cryptography under Visvesvaraya Technological University, India. He has published more than 20 research papers in International Journals, Conferences & Book Chapters and serving as Reviewer for many International Journals and Conferences. He has been conferred with best research contribution award from IEEE ICECCT 2017. His research interest includes Cryptography, Steganography, Digital Image Watermarking and Image Processing.

Dr. L Basavaraj received Bachelor of Engineering (B.E) Degree in Electrical & Electronics Engineering from University of Mysore, India, Master of Technology (M.Tech) Degree in Digital Electronics from Darwad University, India and Doctoral Degree (Ph.D) in the field of Image & Signal Processing under University of Mysore, India. He has published more than 40 research papers in International Journals, Conferences & Book Chapters and currently guiding 7 Ph.D scholars. Being senior member of IEEE, his research interest includes Image & Signal Processing.