SECURE IMAGE STEGANOGRAPHY USING CRYPTOGRAPHY AND IMAGE TRANSPOSITION

Khan Muhammad¹, Jamil Ahmad², Muhammad Sajjad³, Muhammad Zubair⁴

ABSTRACT

Information security is one of the most challenging problems in today's technological world. In order to secure the transmission of secret data over the public network (Internet), various schemes have been presented over the last decade. Steganography combined with cryptography, can be one of the best choices for solving this problem. This paper proposes a new steganographic method based on gray-level modification for true colour images using image transposition, secret key and cryptography. Both the secret key and secret information are initially encrypted using multiple encryption algorithms (bitxor operation, bits shuffling, and stego key-based encryption); these are, subsequently, hidden in the host image pixels. In addition, the input image is transposed before data hiding. Image transposition, bits shuffling, bitxor, stego key-based encryption, and gray-level modification introduce five different security levels to the proposed scheme, making the data recovery extremely difficult for attackers. The proposed technique is evaluated by objective analysis using various image quality assessment metrics, producing promising results in terms of imperceptibility and security. Moreover, the high quality stego images and its minimal histogram changeability, also validate the effectiveness of the proposed approach.

Keywords: cryptography; information security; image processing; image steganography; objective analysis; secret key.

1. INTRODUCTION

Steganography is the process of writing covert messages so that its existence cannot be detected using human visual system (HVS) [1, 2]. The most important prerequisites of steganography include an input image, secret information and data hiding algorithm. To increase the security up to some extent, sometimes a stego key and encryption procedure is also used along with steganographic algorithm. Steganography can be used for a number of different applications including secure exchange of top-secret messages between sensitive organisations, securing online banking, and voting systems [3-6]. It can be one of the most nefarious ways for attackers to send viruses and Trojan horses. Furthermore, terrorists and criminals can use it for secret communication. A number of different steganographic techniques based on carrier object exists including text based

¹ PhD student, Digital Contents Research Institute, Sejong University, Seoul, Korea, Ph. +82-010-48312104, Fax: +82-02-3408-4339, Email: khanmuhammad@sju.ac.kr.
² PhD student, Digital Contents Research Institute, Sejong University, Seoul, Korea, Ph. +82-010-47862016, Fax: +82-02-3408-4339, Email: jamilahmad@sju.ac.kr.
³ Research Associate, Islamia College Peshawar, Pakistan, Ph. +92-333-9319519, Fax: +82-02-3408-4339, Email: Muhammad.sajjad@icp.edu.pk.
⁴ Lecturer, Department of Computer Science, Islamia College Peshawar, Pakistan, Ph. +92-333-93131479, Fax: +82-02-3408-4339, Email: zubair@icp.edu.pk.

Manuscript received on 18th February 2015, reviewed and accepted on 22nd June 2015 as per publication policies of NED University Journal of Research. Pertinent discussion including authors’ closure will be published in September 2016 issue of the Journal if the discussion is received by 28th February 2016.
Khan Muhammad received his Bachelors in computer science from Islamia College, Peshawar, Pakistan in 2014. He is studying PhD in digital contents at Sejong University, Seoul, South Korea. His research interests include image processing, data hiding, steganography, watermarking and video summarization.

Jamil Ahmad received his Bachelors and Masters in computer science, respectively, from the University of Peshawar, Pakistan and Islamia College, Peshawar, Pakistan. He is studying PhD in digital contents at Sejong University, Seoul, Korea. His research interests include image analysis, semantic image representation and content based multimedia retrieval.

Muhammad Sajjad is a Research Associate at Islamia College, Peshawar, Pakistan. He received his PhD in digital contents from Sejong University, Seoul, South Korea. His research interests include digital image super-resolution and reconstruction, sparse coding, video summarisation and prioritisation, image/video quality assessment, and image/video retrieval.

Muhammad Zubair is a Lecturer in the Department of Computer Science at Islamia College, Peshawar, Pakistan. He received his Bachelors in computer science from University of Peshawar, Pakistan in 2009. His research interests include network security, image processing, quality of service and IP based routing.

methods, image steganographic methods, video and audio based data hiding and network packets based data hiding schemes. [1, 7, 8].

Steganographic techniques are divided into the following two categories.

1) Spatial domain techniques which are direct modification of input image's pixels including least significant bit (LSB) methods [9-12], edges based methods [13-17], pixel-value-differencing (PVD) based methods[18, 19], and pixel-indicator-techniques (PIT) [20-27]. These methods result in high quality stego images and provide higher payload but are vulnerable to different normal attacks such as joint photographic experts group (JPEG) compression, noise attacks, and low-pass/high-pass filtering [28] and geometric attacks such as image resizing, cropping and rotations by different angles [29, 30].

2) Transform domain techniques use the transformed-coefficients of the input image obtained through different transforms such as discrete Fourier transform (DFT) [31], discrete wavelet transform (DWT) [32], discrete cosine transform (DCT) [33, 34] and contourlet transform [35] for data hiding. These methods have lower payload but can survive against different attacks.

In this area of steganography, two different groups are working. The first group designs steganographic algorithms while the second group develops its counter attacks (steganalysis). Steganalysis is the science of defeating steganography in a battle that will not end at all. It can be active when the embedded data is to be retrieved. Alternatively, it can be passive where the interest is in detecting the secret information. Detecting the steganography is an important issue for law enforcement authorities as criminals and terrorists mostly use steganography for information interchange [4, 5, 36, 37].

In this paper, a new colour image steganographic technique has been proposed for information hiding. Colour image has been used as a carrier object because it contains more redundant bits. The main contributions of this research work are as follows

1) A new image steganographic technique using gray-level modification and cryptography.
2) Better quality of stego images as compared to other state-of-the-art techniques, verified by experimental results, reducing the chances of detection by adversaries.
3) Encryption of secret key and secret data before data hiding, increasing the security.

The rest of the paper is organized as follows. In section 2, some well-known steganographic techniques are briefly described that are related to the proposed work. Section 3 explains the proposed work in detail, followed by experimental results and discussion in section 4. The conclusion of the paper and future suggestions are presented in section 5.

2. LITERATURE REVIEW

The usage of steganography was started by Greeks with the famous story of shaved head. Over the last few decades, different techniques have been used for message hiding such as tablets with wax, microdots, invisible ink, semagrams, and open codes. In digital steganography, the basic technique of data hiding is to replace the LSBs of the input image with the bits of secret data as described in [38] and its basic idea is given as under

82
Binary representation of eight (8) pixels: 10001101, 10000010, 01110110, 01100001, 00101000, 10000100, 01001011, 01110111.

Secret character: A 01000001

After hiding this secret character (A) in these pixels, the pixel values in binary format are obtained as follows: 10001100, 10000011, 01110110, 01100000, 00101000, 10000100, 01001010, 01110111.

The bold face LSBs indicate the changed pixels during data hiding. It can be seen in the above example that only four pixels change which shows approximately half of the pixels change. Therefore, the distortion caused by this approach in stego images is almost undetectable using HVS.

LSB matching (LSB-M) [17] is a modified version of LSB method which adds/subtracts unity to/from the pixel value if its LSB is not identical to a given secret bit. The asymmetric artifacts produced by LSB method and LSB-M method are reduced by LSB-M revisited (LSB-MR) [12]. Also LSB-MR method interprets the pixel values dependently by considering the relationship between nearby pixels and minimizes the modification rate from 0.5 to 0.325 in the unit bits per pixel (bpp). The extraction of secret data embedded through LSB, LSB-M and LSB-MR is relatively easy for an attacker which is one of the shortcomings of these methods.

To make the extraction of data difficult for attackers, the authors in [39] proposed stego colour cycle (SCC) method that scatters secret data in three channels of the input cover image in a cyclic order. The data is embedded in the sequence of red, green, blue and so on. SCC is further improved by authors in [8] using randomisation. The aforementioned algorithms are better than LSB, LSB-M and LSB-MR methods as it scatters the secret data in different channels of the input cover image. Nevertheless, successfully extracting data from a few pixels can compromise these methods.

Karim et al. [40] proposed a new approach to enhance the robustness of existing LSB substitution method by adding one level security of secret key. In the proposed method, secret key and red channel are used as an indicator while green and blue channels are used as data channels. On the basis of secret key bits and red channel LSBs, the secret data bits are embedded either in green channel or blue channel. An intruder cannot easily extract the secret information without the correct secret key. Moreover, the experimental results also show better image quality and robustness.

The methods discussed so far produce stego images of low quality which are easily detectable using HVS. Furthermore, the data is embedded in cover images without encryption which makes its extraction easy for attackers. This presented research work solves these problems and proposes a new scheme which improves the quality of stego images in addition to increasing the security of secret data during transmission.

3. THE PROPOSED METHODOLOGY

The proposed method is a new robust approach to map secret data to one of the three channels of the red, green and blue (RGB) image. The proposed method uses the idea of transposition, bitxor, bits shuffling, secret key, and cryptography to design an advanced steganographic system. Unlike other methods, the proposed method have the following multiple security levels.

1) All the three channels of the input carrier image are transposed before they can be used to map secret data in order to deceive the attacker.
2) The secret key and secret data is encrypted using multiple encryption algorithms that are applied on it one after another.
3) Secret data is mapped to blue channel of the carrier image using gray-level modification method (GLM) method.

The proposed method uses two different modules named as encryption module and mapping module in order to hide secret data to the carrier image pixels. The overall diagrammatic representation of the proposed framework is shown in Figure 1. The modules of the proposed algorithm are briefly discussed in the forthcoming sections.

3.1 Encryption Module

This module is responsible to encrypt both the secret key and secret data. The final output of this module is secret key and secret data bits in encrypted form. This module performs the following operations on secret key and secret data.
Figure 1. Overall pictorial representation of proposed framework.

1) Select the secret data and a suitable secret key for encryption
2) Convert the secret key into one-dimensional (1-D) array of bits
3) Apply the bitxor operation on these bits with logical 1.
4) Shuffle these encrypted bits such that the bits with even and odd indices are interchanged.
5) If secret key bit = 1

   Then perform bitxor operation of secret message bit with logical 1.
   Else
   Do not perform bitxor operation.
   End if

6) Repeat step 5 until all secret data bits are encrypted.

3.2 Mapping Module

This module is responsible for mapping the secret encrypted data into the carrier image pixels. Before mapping, the carrier image channels are transformed and then a 1-1 mapping between secret data bits and image pixels is maintained. The end result of this module is a stego image, containing secret information.

3.3 Embedding Algorithm

Input: Cover colour image, secret key, and secret data

Output: Stego image

1) Select the colour cover image and divide it into red, green, and blue channels
2) Apply image transpose on all the three channels of the input image
3) Encrypt the secret key and secret data according to the encryption module 3.1
4) If the first bit of secret data = 1
Then convert all pixel values of blue channel to odd by adding 1
Else
Convert all pixel values of blue channel to even by adding 1
5) Map the secret data of step 4 based on secret key bits (SKB) such that
   If SKB=0 && pixel value=even OR SKB=1 && pixel value=odd
       Then leave the pixel unchanged
   Else if SKB=0 && pixel value=odd
       Then subtract 1 from pixel value
   Else if SKB=1 && pixel value=even
       Then add 1 to pixel value
6) Repeat step 5 until all secret bits are mapped with the gray-levels of carrier image
7) Take the transpose of all three planes and combine them to make the stego image

3.4 Extraction Algorithm

   Input: Stego image, secret key
   Output: Secret data
1) Select the colour stego image and divide it into red, green, and blue channels
2) Apply image transpose on all the three channels of the stego image
3) Extract LSB of the blue channel
4) Repeat step 3 until all secret bits are successfully extracted
5) Decrypt these bits by applying the reverse method of encryption module 3.1 to get the original text

4. EXPERIMENTAL RESULTS AND ANALYSIS

This section presents the experimental results based on various image quality assessment metrics for performance evaluation. The proposed method is compared with the Karim et al. method [40] and are implemented using MATLAB R2013a. The evaluation is done using multiple experiments from different perspectives on different standard colour images of varying dimensions. For example, one experiment is to embed a text file of eight kilobyte (8KB) in different standard colour images of dimension (256×256) like Lena, baboon, peppers, army, airplane, building and house. Another experiment is to embed different amount of data in one standard image of the same dimension. The third experiment is to embed the same amount of data in the same image but with different dimensions. For comparison of the proposed method with the existing methods, both the subjective and objective measurements have been used. HVS is a subjective measurement for identification of obvious distortion in the stego images by naked eye [41]. Figure 2-5 show some sample standard colour cover images, stego images and their histograms. Using HVS, it can be noted in Figure 2-5 that the cover and stego images and their histograms are indistinguishable from one another.

![Figure 2. Army tank input and output image with their histograms.](image-url)
Figure 3. Lena input and output image with their histograms.

Figure 4. Baboon input and output image with their histograms.

Figure 5. Peppers input and output image with their histograms.
Objective analysis has also been used for comparison of proposed method with other methods by calculating the normalized-cross-correlation (NCC), peak-signal-to-noise ratio (PSNR), mean square error (MSE) and root MSE (RMSE). Moreover, to show the better performance of the proposed method, histograms changeability and comparison graphs are also mentioned. PSNR, MSE, RMSE and NCC were calculated by the formulae as given in Eqs. (1)-(4) [2, 42].

\[
PSNR = 10 \log_{10} \left( \frac{C_{\text{max}}^2}{MSE} \right)
\]

\[
MSE = \frac{1}{MN} \sum_{x=1}^{M} \sum_{y=1}^{N} (S(x, y) - C(x, y))^2
\]

\[
RMSE = \sqrt{MSE}
\]

\[
NCC = \frac{\sum_{x=1}^{M} \sum_{y=1}^{N} (S(x, y) \times C(x, y))}{\sum_{x=1}^{M} \sum_{y=1}^{N} (S(x, y))^2}
\]

where \(x\) and \(y\) are the loop counters; \(M\) and \(N\) are image dimensions; \(C_{\text{max}}\) is the maximum value among all pixels of both cover and stego images; \(S\) is the stego image; and \(C\) shows the cover image [7, 43, 44].

The experimental results of the proposed algorithm and the Karim et al. [40] algorithm are given in Tables 1-4. The PSNR, MSE, and RMSE scores for both methods have been provided in Table 1. The stego images having PSNR value greater than forty decibel (40dB) are considered to be of high quality. However, PSNR score smaller than 30dB represents lower quality of stego images and hence causes noticeable deformation in stego images which is easily detectable by human visual system. The PSNR values for the proposed algorithm are greater than the Karim et al. [40] algorithm which shows high quality of stego images. Similarly, the MSE values of the proposed algorithm are small as compared to the Karim et al [40] method. Furthermore, the RMSE scores of proposed method are smaller than the Karim et al. [40] method. This means that the proposed algorithm provides promising results in terms of PSNR, confirming its better performance.

The comparison graph of the proposed method and the Karim et al. [40] method is shown in Figure 6. The graph is drawn on the basis of fifteen different smooth and edgy images. The PSNR values are shown on the y-axis and image names on the x-axis. The graph clearly shows that there is up and

<table>
<thead>
<tr>
<th>S. No</th>
<th>Image name</th>
<th>Karim et al. [40] method</th>
<th>Proposed method</th>
<th>Karim et al. [40] method</th>
<th>Proposed method</th>
<th>Karim et al. [40] method</th>
<th>Proposed method</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>PSNR (dB)</td>
<td></td>
<td>MSE</td>
<td>RMSE</td>
<td>MSE</td>
<td>RMSE</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Baboon</td>
<td>50.8811</td>
<td>58.0648</td>
<td>0.5121</td>
<td>0.4487</td>
<td>0.7156</td>
<td>0.6698</td>
</tr>
<tr>
<td>2</td>
<td>Lena</td>
<td>55.6551</td>
<td>58.0362</td>
<td>0.4682</td>
<td>0.4490</td>
<td>0.6842</td>
<td>0.6700</td>
</tr>
<tr>
<td>3</td>
<td>Peppers</td>
<td>17.3893</td>
<td>58.0362</td>
<td>1.4984</td>
<td>0.4490</td>
<td>1.2240</td>
<td>0.6700</td>
</tr>
<tr>
<td>4</td>
<td>Building</td>
<td>55.1595</td>
<td>59.3242</td>
<td>0.4724</td>
<td>0.4392</td>
<td>0.6873</td>
<td>0.6627</td>
</tr>
<tr>
<td>5</td>
<td>Parrot</td>
<td>41.9414</td>
<td>59.3242</td>
<td>0.6212</td>
<td>0.4392</td>
<td>0.7881</td>
<td>0.6627</td>
</tr>
<tr>
<td>6</td>
<td>Army</td>
<td>55.6788</td>
<td>60.3252</td>
<td>0.4680</td>
<td>0.4319</td>
<td>0.6841</td>
<td>0.6571</td>
</tr>
<tr>
<td>7</td>
<td>Office</td>
<td>45.3351</td>
<td>58.3514</td>
<td>0.5747</td>
<td>0.4465</td>
<td>0.7580</td>
<td>0.6682</td>
</tr>
<tr>
<td>8</td>
<td>F16jet</td>
<td>47.335</td>
<td>58.0576</td>
<td>0.5505</td>
<td>0.4488</td>
<td>0.7419</td>
<td>0.6699</td>
</tr>
<tr>
<td>9</td>
<td>House</td>
<td>50.949</td>
<td>58.1054</td>
<td>0.5114</td>
<td>0.4484</td>
<td>0.7151</td>
<td>0.6696</td>
</tr>
<tr>
<td>10</td>
<td>Building1</td>
<td>28.7007</td>
<td>58.0116</td>
<td>0.9078</td>
<td>0.4491</td>
<td>0.9527</td>
<td>0.67014</td>
</tr>
<tr>
<td>11</td>
<td>Trees1</td>
<td>38.7399</td>
<td>58.1752</td>
<td>0.6726</td>
<td>0.4479</td>
<td>0.8201</td>
<td>0.6692</td>
</tr>
<tr>
<td>12</td>
<td>Trees2</td>
<td>24.0736</td>
<td>58.0284</td>
<td>1.0823</td>
<td>0.4490</td>
<td>1.0403</td>
<td>0.6700</td>
</tr>
<tr>
<td>13</td>
<td>Girl1</td>
<td>28.3517</td>
<td>58.1558</td>
<td>0.9190</td>
<td>0.4480</td>
<td>0.9586</td>
<td>0.6693</td>
</tr>
<tr>
<td>14</td>
<td>Girl2</td>
<td>55.9034</td>
<td>58.1872</td>
<td>0.4661</td>
<td>0.4478</td>
<td>0.6827</td>
<td>0.6691</td>
</tr>
<tr>
<td>15</td>
<td>Girl3</td>
<td>50.1731</td>
<td>59.595</td>
<td>0.5193</td>
<td>0.4372</td>
<td>0.7206</td>
<td>0.6612</td>
</tr>
<tr>
<td>Average</td>
<td>40.5017</td>
<td>58.5185</td>
<td>0.6829</td>
<td>0.4453</td>
<td>0.8115</td>
<td>0.6673</td>
<td></td>
</tr>
</tbody>
</table>
Table 2. Comparison of methods using PSNR with variable amount of embedded cipher

<table>
<thead>
<tr>
<th>Image name</th>
<th>Cipher size in (Kbs)</th>
<th>Cipher size in bytes</th>
<th>Karim et al. [40] method PSNR (dB)</th>
<th>Proposed method PSNR (dB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>baboon with dimension 256×256</td>
<td>2</td>
<td>2406</td>
<td>19248</td>
<td>52.0373</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>4177</td>
<td>33416</td>
<td>51.6345</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>6499</td>
<td>51992</td>
<td>51.1776</td>
</tr>
<tr>
<td></td>
<td>8</td>
<td>8192</td>
<td>65536</td>
<td>50.8811</td>
</tr>
</tbody>
</table>

Table 3. Comparison of both methods using PSNR with variable image dimensions

<table>
<thead>
<tr>
<th>Image name</th>
<th>Cipher embedded (bits)</th>
<th>Image dimensions</th>
<th>Karim et al. [40] method PSNR (dB)</th>
<th>Proposed method PSNR (dB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>baboon</td>
<td>1720</td>
<td>128×128</td>
<td>65.5328</td>
<td>67.9197</td>
</tr>
<tr>
<td></td>
<td>1720</td>
<td>256×256</td>
<td>50.8811</td>
<td>74.1737</td>
</tr>
<tr>
<td></td>
<td>1720</td>
<td>512×512</td>
<td>37.2456</td>
<td>88.0026</td>
</tr>
<tr>
<td></td>
<td>1720</td>
<td>1024×1024</td>
<td>41.9577</td>
<td>85.8083</td>
</tr>
</tbody>
</table>

Table 4. Comparison of both methods using NCC with different images

<table>
<thead>
<tr>
<th>Serial No</th>
<th>Image Name</th>
<th>Karim et al. [40] Method NCC</th>
<th>Proposed Method NCC</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Baboon</td>
<td>0.9998</td>
<td>0.9999</td>
</tr>
<tr>
<td>2</td>
<td>Lena</td>
<td>0.9999</td>
<td>0.9999</td>
</tr>
<tr>
<td>3</td>
<td>Peppers</td>
<td>0.7859</td>
<td>0.9093</td>
</tr>
<tr>
<td>4</td>
<td>Building</td>
<td>0.9999</td>
<td>0.9999</td>
</tr>
<tr>
<td>5</td>
<td>Parrot</td>
<td>0.9991</td>
<td>0.9995</td>
</tr>
<tr>
<td>6</td>
<td>Army</td>
<td>0.9999</td>
<td>0.9999</td>
</tr>
<tr>
<td>7</td>
<td>Office</td>
<td>0.9998</td>
<td>0.9999</td>
</tr>
<tr>
<td>8</td>
<td>F16jet</td>
<td>0.9997</td>
<td>0.9998</td>
</tr>
<tr>
<td>9</td>
<td>House</td>
<td>0.9998</td>
<td>0.9999</td>
</tr>
<tr>
<td>10</td>
<td>Building1</td>
<td>0.9796</td>
<td>0.9899</td>
</tr>
<tr>
<td>11</td>
<td>Trees1</td>
<td>0.9989</td>
<td>0.9994</td>
</tr>
<tr>
<td>12</td>
<td>Trees2</td>
<td>0.9721</td>
<td>0.9897</td>
</tr>
<tr>
<td>13</td>
<td>Girl1</td>
<td>0.9809</td>
<td>0.9898</td>
</tr>
<tr>
<td>14</td>
<td>Girl2</td>
<td>0.9999</td>
<td>0.9999</td>
</tr>
<tr>
<td>15</td>
<td>Girl3</td>
<td>0.9998</td>
<td>0.9999</td>
</tr>
<tr>
<td>Average</td>
<td></td>
<td>0.981</td>
<td>0.9917</td>
</tr>
</tbody>
</table>

Figure 6. Comparative Analysis of both methods using PSNR with different images.
down in the values of PSNR of the Karim et al. [40] method but the values of PSNR in the proposed method are almost the same and do not vary significantly. This verifies that the proposed method performs well for all types of images (edgy and smooth) as compared to the Karim et al. [40] method.

Table 2 shows the comparison of both methods using PSNR with variable amount of cipher that is embedded in the standard colour image (baboon) of the same dimension (256×256). Table 2 clearly shows that the proposed method gives more PSNR score as compared to the Karim et al. [40] method. Similarly, the comparative analysis graph of both the methods with variable amount of cipher embedded in a standard colour image of the same dimension is shown in Figure 7. The graph is drawn on the basis of PSNR values of Table 2. The comparative graph of the proposed algorithm as compared to the Karim et al. [40] algorithm clearly shows its better results in terms of PSNR which validate the effectiveness of the proposed method.

Table 3 provides the comparison of both methods using PSNR with the same amount of cipher embedded and same standard image (baboon) but with different dimensions. The results of Table 3 show that there is variation in the PSNR score of the Karim et al. [40] method but the PSNR score of the proposed algorithm is increasing as the image size is increased. Similarly, the comparative graph of both methods using PSNR with variable dimensions, same image and same amount of cipher embedded is also shown in Figure 8 which vividly describes the effectiveness of the proposed technique.

The similarity between two images can be measured by using the correlation function. NCC is a statistical error metric that has been used to measure the similarity between two digital images in this research work. Table 4 shows NCC for both the algorithms. If the NCC value is unity, both images become identical to each other. The value of NCC in Table 4 close to unity shows that both the images are similar and differences are small. Table 4 clearly shows that the NCC values for the proposed algorithm in all cases are greater than the Karim et al. [40] algorithm. This shows that the proposed algorithm provide better results in terms of NCC also and verifies its effectiveness.

5. CONCLUSIONS

In this paper, a new method is proposed to map secret data to the gray-levels of the carrier image by utilising the concepts of transposition, bitxoring, bits shuffling, secret key, and cryptography with high imperceptibility and security. An average PSNR of 58dB, RMSE with 0.6673, and NCC with 0.9917 is achieved using the proposed method which are better than the existing method in
the literature with PSNR=40, RMSE=0.8115, and NCC=0.981. The proposed method improved the security as well as the quality of stego images and provided promising results in terms of high PSNR, NCC, and less histogram changeability as compared to existing methods. The distinguishing properties of the proposed algorithm include transposition, bitxorring, and bits shuffling, adding multiple security levels to the proposed method. These different security levels create multiple barriers in the way of an attacker. Therefore, it is difficult for a malicious user to extract the actual secret data.

ACKNOWLEDGMENT

The authors are thankful to the anonymous reviewers, associate editor, and editorial board members for providing their useful and constructive comments which improved the quality of this paper. The authors also acknowledge Dr. Zahoor Jan for his continuous help and support.

REFERENCES


