Dual Level Security Scheme (DLSS)
Using RGB Layer Cryptography and Audio Steganography for Secret Image Transmission in Unsecure Medium

P L Chithra\textsuperscript{1*}, R Aparna\textsuperscript{2}

\textsuperscript{1}Professor, Department of Computer Science, University of Madras, India
\textsuperscript{2}Research Scholar UNOM, Assistant Professor, Department of Information Technology, M.O.P. Vaishnav College for Women, India

Abstract

Objectives: Recent trend depicts a steep hike in the value of data. Data in all forms are vulnerable and especially multimedia data are fascinated by hackers. Hence, strong security measure has to be applied before attempting to use the unsecure transmission medium for sharing secret / personal data. Methods: Dual Level Security Scheme (DLSS) is proposed which combines cryptography and steganography techniques to ensure double level security. Cipher image is obtained by applying Spiral Mapping and discrete cosine transformations (DCT) in RGB Layers. Then, the cipher image is hidden in the audio signal. Findings: SNR value is considered for normalizing the signals before embedding it, to obtain final signal without any traces of the hidden secret signal. Core objective of using DLSS is maintaining the secrecy when data transmission is taking place in any unsafe medium. Simulation results of our proposed method exhibit an average of 10% improvement and hence, DLSS outperforms well over the existing methods. Competence of the method is evident from the performed histogram analysis. Standard image dataset is used and directional correlation, PSNR, SSIM, and MSE are the considered measures to prove DLSS efficiency. Novelty: Here, a novel method Dual Level Security Scheme (DLSS) with spiral mapping is proposed to incorporate the aids of cryptography and steganography for enhanced efficiency.

Keywords: Cryptography; Steganography; RGB Layer Extraction; DCT; Spiral Mapping

1 Introduction

Usually signals in any form are vulnerable to hacking. So, it is not safe to transfer any secret message through unsecure/open medium. But there is always a necessity to communicate secret messages. Hence, it is high time to devise a strong algorithmic technique to support security for transferring secret messages in unsafe medium. In this paper, a novel method (DLSS) has been proposed. DLSS (Dual Level Security Scheme) combines the advantages of two strong techniques, namely, cryptography and...
1. Limitations of the existing methods

- Traditional systems use either crypto or stegano technique for secure data transformation.
- Existing cryptographic methods are limited to the fixed size of the secret images.
- Various mapping techniques are used with high complexity and CPU time.
- Steganography is restricted with hiding secret image in a specific cover image that can accommodate secret image.
- Poor results in performance measures.

1.2 Significance of the proposed DLSS method

- Double protection with crypto or stegano techniques.
- No limitations in choosing the secret image size except to accomplish spiral mapping.
- Very minimal or no restrictions in choosing the cover audio and it perfectly fits for any secret image.
- Spiral Mapping is simple but applied to each layer in the RGB color channel to withstand brute force attack.
- Normalization technique supports in choosing any ordinary audio signal as cover signal without any restrictions.
- As audio signal is a scalar dataset, hiding image in audio allows to choose images of high dimensions.
- Shows improved results in performance measures.
2 Methodology

As the proposed method involves both the cryptographic and steganographic concepts\textsuperscript{(19,21,22)} for strengthening the security, it is called Dual Level Security Scheme (DLSS). Cryptography is the process of converting the plain signal into cipher signal, on the other hand, Steganography is the process of hiding the secret signal in covering signal. Both the methods have their own merits to contribute to our proposed methodology.

2.1 Cryptography

The proposed encryption technique is applied to the RGB layer and transformation\textsuperscript{(1,6)} is also applied to the individually formed datasets. This helps in producing different cipher images for each small change in the original secret image\textsuperscript{(7)}. This RGB layer extraction supports to build a system to sustain the brute force attacks.

2.1.1 RGB Layer Extraction

The input color image is pre-processed and RGB layers are split to form three separate datasets\textsuperscript{(3,4)}. The three datasets are treated as separate matrices. The obtained layers are managed well before ciphering to prevent data loss during encryption. The encryption process is applied to all the three layers separately.

![Fig 1. Spiral Mapping on 3X3 image layers](https://www.indjst.org/)

2.1.2 Spiral Mapping

In the spiral coding scheme, the RGB signal is modulated on a spiral path in the two-dimensional plane. Each RGB matrices are spiral mapped, hence, the diffusion applied is strong and the proposed method shows evident progress in correlation test. The color image comprises three-layer data. Each layer is spiral mapped separately after applying proper transformation. Finding the mid-point of the RGB layer matrices is essential to start with the spiral mapping. The mid-point is calculated from the size of the secret image taken. Having set the mid-point, all the pixels are shuffled. This process is performed on each of the three RGB layer matrices. Hence, three separated diffused dataset is obtained and it is combined to form the final cipher image. Figure 1 shows the shuffling pattern of each of the RGB layer matrices. As shown in Figure 2, it is obvious that approximately only one pixel remains unchanged and the rest of the other pixels are shuffled well.

2.1.3 RGB Layer Cosine Transformation

A color image basically has three values /channels per pixel and they are used to measure the intensity and chrominance of light. The brightness information in each spectral band is the actual information stored in the digital image data. To perform RGB layer cosine transformations, the secret signal in the form of color image has to be first pre-processed and split into three different matrices referring to each color channel.

Discrete Cosine Transformation (DCT) is a technique for converting a signal into elementary frequency components\textsuperscript{(16,17)}. The transformed array obtained through DCT is also of the size N x N, same as that of the original image block. Discrete Cosine Transformation (DCT) of each layer is obtained separately and well maintained. Color layer segmentation is performed with extra attention to avoid any color data leakage. Data loss in this stage may also affect the performance measure and
effectiveness of the proposed system. Although DFT is used in many systems, here DCT is applied. As the signal is represented periodically, the signal will tend to lose its original form while truncating representation coefficients in DFT. In DCT, the signal can withstand relatively more coefficient truncation due to its periodic structure. Hence, DCT is used here and its formula is given in eqn. (1). And Inverse DCT is applied in the receiver’s end to revert back the secret image signal from the encrypted dataset. Transformation plays a vital part in encryption and decryption, hence, should be performed lossless to obtain secret data. The following formula given in eqn (2) is used to calculate the Inverse DCT.

\[
\text{DCT} (u, v) = \alpha (u) \alpha (v) + \sum_{y=0}^{N-1} \left( \sum_{x=0}^{N-1} f(x, y) \cos \left( \frac{\pi (2x+1) u}{2N} \right) \cos \left( \frac{\pi (2x+1) v}{2N} \right) \right) \\
\]

(1)

\[
f (x, y) = \sum_{v=0}^{N-1} \left( \sum_{u=0}^{N-1} \alpha (u) \alpha (v) \text{DCT} (u, v) \cos \left( \frac{\pi (2x+1) u}{2N} \right) \cos \left( \frac{\pi (2x+1) v}{2N} \right) \right)
\]

(2)

for \( u, v = 0, 1, 2, \ldots \ldots, N-1 \), \( \alpha (u) = \begin{cases} 
\sqrt{\frac{1}{N}} & \text{for } u = 0 \\
\sqrt{\frac{1}{N}} & \text{for } u \neq 0 
\end{cases} \)

\( \alpha (v) = \begin{cases} 
\sqrt{\frac{1}{N}} & \text{for } v = 0 \\
\sqrt{\frac{2}{N}} & \text{for } v \neq 0 
\end{cases} \)

2.1.4 Steganography

Steganography is the next pillar for this proposed DLSS method, which aims at hiding the cipher image signal in the audio signal without leaving any traces of hidden signal. The encrypted image has to be converted into 1D scalar dataset. To hide the cipher image data into an unsuspicious ordinary audio file, the size of the obtained cipher image should be altered. The secret image and covering audio file need not have any relations; this makes the proposed system suitable for any image file. The audio signal can also be chosen by the parties involved in covert transmission. The size of the obtained 1D dataset of the image is adjusted by appending null values.

https://www.indjst.org/
2.1.5 Correlation Extemporization by Normalization

Correlation test in steganography is to prove the minimal or no change in the covering signal, even after embedding the encrypted 1D dataset of the secret image. The normalization factor \( f(n) \) is calculated as follows,

\[
Encryption f(n) = \begin{cases} 
    n \in N; \frac{\text{SNR}(S1)}{n} = \text{SNR}(S2) & \\
    0, \text{ otherwise} 
\end{cases}
\]

\( 3 \)  

\[
Decryption g(n) = \begin{cases} 
    n \in N; \text{SNR}(S1) \times n = \text{SNR}(S2) & \\
    0, \text{ otherwise} 
\end{cases}
\]

\( 4 \)

where, \( f(n) \) → function to calculate the normalization factor during encryption, 
\( g(n) \) → function to calculate the normalization factor during decryption, 
\( S1 \) → Covering signal after embedding, 
\( S2 \) → Original covering signal

The normalization factor is computed in such a way that there is negligible or no doubt of hidden secret signal in the original covering signal which will be transmitted on unsecure medium. Normalization factor is computed as shown in eqns.(3) and (4) based on the comparison of the SNR value of the signal before and after embedding the secret encrypted dataset.

2.2 Overview of DLSS

![Fig 3. DualLevel Security Scheme](https://www.indjst.org/)
2.1.3. Adjust the Inference to amplify cipher signal
3. Construct the Cipher Image Signal from the 1D signal
4. Cryptography – Decryption Process
4.1. Extract Each Color Layer and Construct 3 Separate RGB Matrices
4.2. IDCT Transformation
4.3. Apply Reverse Spiral Mapping Technique on RGB Matrices
4.4. Merge RGB Matrices into Single Matrix to Obtain Secret Image
5. Secret Image is obtained.

3 Result and Discussion

The proposed methodology is simulated in MATLAB environment with standard secret images and the results are compared with the existing methods. Comparative analysis is performed for cryptography and steganography techniques separately by comparing the measures such as correlation values, PSNR, MSE values and histograms of our results with existing methods. Tables 1, 2, 3 and 4 proves that the DLSS performs well over other methods.

3.1 Correlation Tests

Correlation refers to the strength of the relationship between the selected datasets. The value of the correlation coefficient varies between +1 and -1. Since our proposed DLSS method includes cryptography and steganography, here correlation test is performed in two different aspects. With respect to cryptography, the correlation test is carried out to show the original secret image and the RGB layer spiral mapped encrypted image does not have or have very minimal similarities. Hence, we achieve strong cryptographic method by getting the values closer to -1. The formula for calculation is shown in eqns.(5) and (6). Whereas, in steganography, the correlation test is performed to check whether there is any trace of hidden dataset in the audio signal after embedding the encrypted secret data. So, here the resulting values are proved to be closer to 1.

The coefficient of correlation between the original secret image and the encrypted cipher image is analyzed by computing the correlation between various original and cipher images using the following formula:

\[ r = \frac{\sum_{i=1}^{I} \sum_{j=1}^{J} (x_{ij} - \bar{x})(y_{ij} - \bar{y})}{\sqrt{\sum_{i=1}^{I} \sum_{j=1}^{J} (x_{ij} - \bar{x})^2 \sum_{i=1}^{I} \sum_{j=1}^{J} (y_{ij} - \bar{y})^2}} \]  

(5)

\[ r_{xy} = \frac{\sigma_{xy}}{\sigma_x \sigma_y} \]  

(6)

where x and y are the two datasets for which the cross-correlation (r) is calculated.

<table>
<thead>
<tr>
<th>#</th>
<th>Input Image</th>
<th>Correlation Direction</th>
<th>Horizontal</th>
<th>Vertical</th>
<th>Diagonal</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Plain Lenna</td>
<td></td>
<td>0.9740</td>
<td>0.9868</td>
<td>0.9612</td>
</tr>
<tr>
<td>2</td>
<td>Proposed DLSS Method</td>
<td></td>
<td>-0.0022</td>
<td>0.0053</td>
<td>0.0018</td>
</tr>
<tr>
<td>3</td>
<td>Khan, M., &amp; Waseem, H. M. (1)</td>
<td></td>
<td>-0.0113</td>
<td>-0.0093</td>
<td>0.0027</td>
</tr>
<tr>
<td>4</td>
<td>Yang, B., &amp; Liao, X. (2)</td>
<td></td>
<td>-0.0064</td>
<td>0.0107</td>
<td>0.0051</td>
</tr>
<tr>
<td>5</td>
<td>Teng, L., Wang, X., &amp; Meng, J. (3)</td>
<td></td>
<td>-0.0109</td>
<td>-0.0181</td>
<td>-0.0061</td>
</tr>
</tbody>
</table>

1 and 2 are depicted to prove the strength of the proposed DLSS technique. The horizontal, vertical and diagonal correlation coefficients of the original secret image and the encrypted image are shown in Table 1. The proposed DLSS method produces the correlation coefficient values closer to -1 than the existing methods (1-3). Table 2 shows the correlation coefficient values of the covering audio signal before and after embedding the secret data, which is closer to 1. It proves that there will not be any trace of the hidden secret data.
Table 2. Correlation Comparison of Covering Audio Signal – Steganography

<table>
<thead>
<tr>
<th>#</th>
<th>Cover Audio</th>
<th>Secret Image</th>
<th>Image Size</th>
<th>Before and After Embedding Secret Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>TIMIT corpus</td>
<td>Lenna</td>
<td>512 x 512</td>
<td>0.9987568</td>
</tr>
<tr>
<td>2</td>
<td>Lenna</td>
<td>Lenna</td>
<td>256 x 256</td>
<td>0.9996862</td>
</tr>
<tr>
<td>3</td>
<td>F16</td>
<td>256 x 256</td>
<td>0.9977844</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Baboon</td>
<td>256 x 256</td>
<td>0.998761</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>House</td>
<td>256 x 256</td>
<td>0.9996471</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Trees</td>
<td>256 x 256</td>
<td>0.9996436</td>
<td></td>
</tr>
</tbody>
</table>

3.2 PSNR and SSIM measures

The two measures Peak Signal to Noise Ratio (PSNR) and Structural Similarity Index Measure (SSIM) are used to compare the differences between the original secret image and the encrypted image. PSNR can be calculated by the following equation

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

Here, the PSNR and SSIM values are calculated to show the similarities between the decrypted and original images. MSE is mean square error and the formula is given below.

$$MSE = \frac{1}{mn} \sum_{x=1}^{m} \sum_{y=1}^{n} (D(x,y) - S(x,y))^2$$

where m & n represent the dimensions of the secret image, 
D is the decrypted image and S is the original secret image.

The structural similarity (SSIM) between the images is calculated as follows:

$$SSIM(D,S) = \frac{(2\mu_x\mu_y + P_1)(2\sigma_{xy} + P_2)}{(\mu_x^2 + \mu_y^2 + P_1)(\sigma_x^2 + \sigma_y^2 + P_2)}$$

Fig 4. Plain lenna Image 512X512

Comparison analysis and the performance of the proposed DLSS method are shown in Tables 3 and 4. The high values for PSNR and the SSIM closer to 1 prove the efficiency of the proposed method. Our proposed work exhibits an average of 10% improvement to the existing systems because of the mapping technique used in it. The spiral mapping methodology proposed...
Fig 5. Encrypted lenna Image

Fig 6. Decrypted lenna Image

Fig 7. Plain Baboon Image
here will shuffle the data well without losing any data, hence, helps in better results. Figures 4 and 7 show the original secret image and Figures 5 and 8 show the cipher images. Correlations between the original image and encrypted image generate the values closer to -1, which shows the vast variations between them. Hence, it is the success of the proposed cryptographic method. Figures 6 and 9 show the decrypted images in the receiver side.

Table 3. Comparison of the proposed method with other existing color image schemes

<table>
<thead>
<tr>
<th>#</th>
<th>Image</th>
<th>Proposed Method</th>
<th>DLSS Valandar, M. Y., et. al (9)</th>
<th>Jassim FA (13)</th>
<th>Gutub AA-A et. al. (14)</th>
<th>Muhammad K., et.al. (15)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>F16</td>
<td><strong>60.1274</strong></td>
<td>0.9999</td>
<td>53.7294</td>
<td>0.9999</td>
<td>40.2347</td>
</tr>
<tr>
<td>2</td>
<td>Baboon</td>
<td><strong>61.0083</strong></td>
<td><strong>0.9999</strong></td>
<td>48.5478</td>
<td>0.9998</td>
<td>39.9997</td>
</tr>
<tr>
<td>3</td>
<td>House</td>
<td><strong>60.2182</strong></td>
<td><strong>0.9999</strong></td>
<td>53.2479</td>
<td>0.9997</td>
<td>40.2518</td>
</tr>
<tr>
<td>4</td>
<td>Trees</td>
<td><strong>67.3691</strong></td>
<td><strong>0.9999</strong></td>
<td>49.8697</td>
<td>0.9998</td>
<td>39.5397</td>
</tr>
</tbody>
</table>

The results shown in Table 1 with the correlation values closer to 0 in all directions is the significance of this work. Standard images (such as Lenna, Baboon, House, Trees) are taken as inputs and the correlation values are noted as -0.0022, 0.0053, 0.0018 which are very closer to 0. The correlation tests for steganography are performed and the values are >= 0.999, closer to 1, which
<table>
<thead>
<tr>
<th>#</th>
<th>Plain Image</th>
<th>Image Size</th>
<th>PSNR</th>
<th>SSIM</th>
<th>MSE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Lenna</td>
<td>512 x 512</td>
<td>59.543</td>
<td>0.999965</td>
<td>0.07224</td>
</tr>
<tr>
<td>2</td>
<td>Lenna</td>
<td>256 x 256</td>
<td>60.14874</td>
<td>0.999980</td>
<td>0.01873</td>
</tr>
<tr>
<td>3</td>
<td>F16</td>
<td>256 x 256</td>
<td>60.12744</td>
<td>0.999940</td>
<td>0.01768</td>
</tr>
<tr>
<td>4</td>
<td>Baboon</td>
<td>256 x 256</td>
<td>61.00826</td>
<td>0.999975</td>
<td>0.01379</td>
</tr>
<tr>
<td>5</td>
<td>House</td>
<td>256 x 256</td>
<td>60.21819</td>
<td>0.999952</td>
<td>0.01843</td>
</tr>
<tr>
<td>6</td>
<td>Trees</td>
<td>256 x 256</td>
<td>67.36909</td>
<td>0.999990</td>
<td>0.00175</td>
</tr>
</tbody>
</table>

shows the effective hiding of cipher data in the audio signal. PSNR values $\geq 60$ and minimal Mean Square Error (MSE) is recorded showing the overall performance of DLSS.

### 3.3 Histogram Analysis

Histogram analysis is performed to exhibit the security of the proposed DLSS method. Histogram analysis shows the way in which pixels in RGB image are spread by denoting the number of pixels at each intensity level [8]. Figure 10, displays histogram of the original secret image and the histogram of the cipher image is shown in Figure 11. The cipher image histogram is totally different from the histogram of the original secret image and it is peculiar in statistical similarity, which clearly proves that no information about the original image can be obtained from cipher image. Hence, histogram analysis is carried to prove the efficiency of the proposed DLSS method. At the same time, histogram of the decrypted image is similar in visual effect of the original secret image histogram, which is shown in Figure 12 proves that the original image can be completely recovered without any loss of information.
4 Conclusion

Secret data need to be safeguarded to prevent data theft. Providing security deals with encryption and encoding. In spite of applying strong cryptographic algorithm, inclusion of steganographic method enhances the novelty of the proposed work. The proposed spiral mapping scheme on RGB layer of the secret image is less complex and out performs well over the existing methods. Incorporation of crypto with stegano techniques ensures secure transmission of secret image in unsafe open medium. Correlation coefficients are derived to prove the similarities between original secret image and decrypted image and audio signals before and after embedding. Simulation results of our proposed method exhibit an average of 10% improvement and the significant improvement in PSNR which is greater than 60, SSIM closer to 1 and negligible MSE measures prove the
lossless transmission of secret image. Thus, the proposed DLSS method, a combined approach of crypto and stegano shows high performance rate than the existing methods.

References