INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

RESEARCH ARTICLE

OPEN ACCESS

Received: 29-04-2023

Accepted: 24-05-2023

Published: 13-06-2023

Citation: Chithra PL, Aparna R (2023) Dual Level Security Scheme (DLSS) Using RGB Layer Cryptography and Audio Steganography for Secret Image Transmission in Unsecure Medium. Indian Journal of Science and Technology 16(23): 1733-1744. https://doi.org/10.17485/IJST/v16i23.924

* **Corresponding author**.

chitrasp2001@yahoo.com

Funding: None

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

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

P L Chithra[1]*, **R Aparna**[2]

1 Professor, Department of Computer Science, University of Madras, India
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 steganography.

Data in the form of color image signals often draw the attention of intruders and hackers. This seriously affects the security of the data. Hence, the proposed method helps in safeguarding secret data which are in the form of color images. The coordinate values of each pixel in secret image signal are extracted and encrypted to form the cipher image. Color image is considered the input and separate datasets are formed for each RGB specifications. The devised spiral mapping on each layer followed by RGB layer cosine transformation produces encrypted cipher image. The cipher image itself holds acceptable strength towards intruding prevention. Next, the cipher image is hidden inside the speech signal without the evidence of hidden data. Although the cipher image is strong enough to withstand hackers' attacks, the inclusion of steganographic concept still enhances the novelty of the proposed DLSS method. Standard measures such as correlation coefficients, PSNR, SSIM and MSE are calculated to portray the efficiency of the proposed DLSS method. Correlations are used to show the vast difference between the original and cipher images. The process of embedding is proved with correlation measure, since the value is closer to 1, shows the similarities of the covering audio signal before and after embedding. PSNR, SSIM and MSE measures are calculated to provide evidence for the similarities between the cipher and original secret image in the receiver end. Standard color images are involved for proving the level of the system. Audio file can be chosen by the sender and receiver accordingly, which makes the proposed method withstand the intruder's attacks.

Image encryption scheme based on quantum dynamical spinning and rotations [1], by Khan, M., & Waseem H. M. elaborates the need for newer techniques to accompany secrecy in quantum computing. The advantage of quantum information processing in cyber security is also absorbed. Color image encryption schemes [2,3] present various techniques to affix protection to image data. Chaotic systems and their applications in image encryption [3–5] provide advantages of random behavior and resistance to brute force attacks. The limited computation, memory and communication capabilities make the chaotic system not suitable for larger size images. In color image, every pixel consists of RGB color components that determine the intensity of the color in the image [1,6,7]. There are a variety of encryption schemes available and it is essential to identify the appropriate technique to be implemented. Histogram is the graphical representation of digital image which plots the number of pixels for each tonal value [8]. Considering the image intensities [8] in encoding process enhances the system. Mapping is a well-known technique adapted in encryption scheme. In this paper, spiral mapping method is proposed for RGB layer image encryption. Various mapping methods are available and each has its own pros and cons. Cat mapping, Duffing map, logistic map, and 3D chaotic mapcan also be used in diffusion process of image encryption. The working of various cryptographic algorithms is viewed and the DLSS algorithm is proposed to overcome their disadvantages. Securing data by hiding it within another signal [9,10] is proved to be a traditional method with high success rate. A deep understanding of the color image shuffling and encoding techniques are essential to propose a strong methodology. Various steganographic methods [11–14] are available to ensure security. Recent researches shows transformations of secret image data aids to handle the signal [15–20] more efficiently and hide into cover audio signal [19]. Crypto-Stegano approaches incorporates various algorithms respectively to adapt domain secret images [21,22]. Based on the analysis of various existing approaches and recent methodologies, the secure DLSS scheme is proposed to enhance the security.

1.1 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 [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 [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 [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 [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.

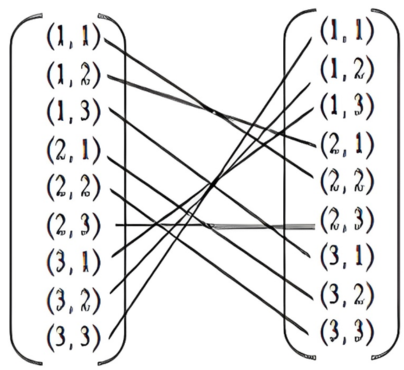

Fig 1. Spiral Mapping on 3X3 image layers

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 [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

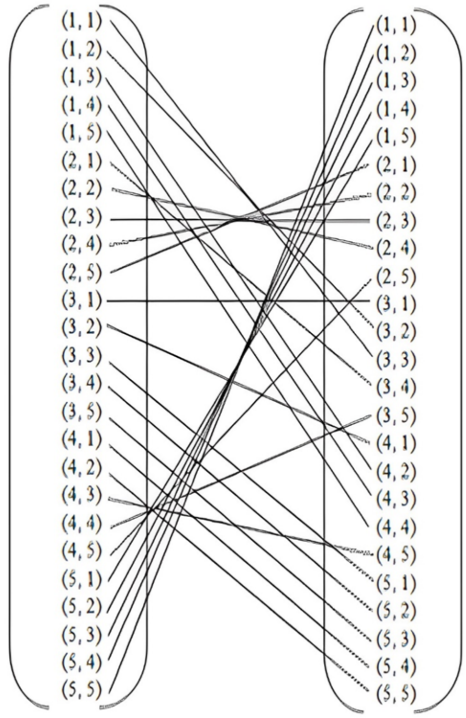

Fig 2. Spiral Mapping on 5X5 image layers

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.

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

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

for u,v = 0,1,2……..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.

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 [19] is calculated as follows,

$$Encryption f(n) = \begin{cases} n \in N, \dfrac{SNR(S1)}{n} = SNR(S2) \\ 0, \text{ otherwise} \end{cases} \quad (3)$$

$$Decryption g(n) = \begin{cases} n \in N, SNR(S1) * n = SNR(S2) \\ 0, \text{ otherwise} \end{cases} \quad (4)$$

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

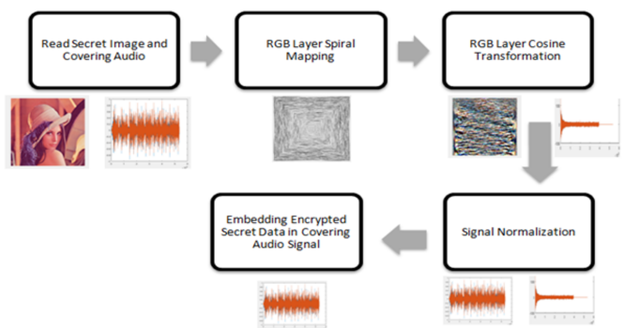

Fig 3. DualLevel Security Scheme

2.2.1 Dual Level Security Scheme

2.2.1.1 Sender - side Processing. 1. Read Secret Image & Cover Audio
2. Cryptography
2.1.1. Extract Each Color Layer and Construct 3 Separate RGB Matrices
2.1.2. DCT Transformation
2.1.3. Apply Spiral Mapping Technique on RGB Matrices
2.1.4. Merge RGB Matrices into Single Matrix to Obtain Cipher Image
3. Convert the Cipher Image dataset into 1D signal
4. Steganography
4.1. Adjust 1D signal to Cover Audio Size
4.2. Apply Normalization Mechanism to Adjust Inference
4.3. Embed Cipher Image Data in the Cover Audio
5. Send the processed Audio Signal in any unsecure medium

2.2.1.2 Receiver - side Processing. 1. Read the received Audio Signal
2. Steganography – Unbounding Process
2.1.1. Read the Cover Signal
2.1.2. Extract Cipher Image Data from the received Audio

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 [2,19] 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:

$$r = \frac{\sum_{i=1}^{I} 1\sum_{j=1}^{J}\left(x_{ij}-\bar{x}\right)\left(y_{ij}-\bar{y}\right)}{\sqrt{\left(\sum_{i=1}^{I} 1\sum_{j=1}^{J}\left(x_{ij}-\bar{x}\right)^{2}\right)\left(\sum_{i=1}^{I} 1\sum_{j=1}^{J}\left(y_{ij}-\bar{y}\right)^{2}\right)}} \tag{5}$$

$$r_{xy} = \frac{\sigma_{xy}}{\sqrt{\sigma_x^2\sigma_y^2}} \tag{6}$$

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

Table 1. Correlation comparison of the proposed method with other existing methods

#	Input Image	Correlation Direction		
		Horizontal	Vertical	Diagonal
1	Plain Lenna	0.9740	0.9868	0.9612
2	Proposed DLSS Method	-0.0022	0.0053	**0.0018**
3	Khan, M., & Waseem, H. M. [1]	-0.0113	-0.0093	0.0027
4	Yang, B., & Liao, X. [2]	-0.0064	0.0107	0.0051
5	Teng, L., Wang, X., & Meng, J. [3]	-0.0109	-0.0181	-0.0061

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

#	Cover Audio	Secret Image	Image Size	Before and After Embedding Secret Data
1	TIMIT corpus	Lenna	512 x 512	0.9987568
2		Lenna	256 x 256	0.9996862
3		F16	256 x 256	0.9977844
4		Baboon	256 x 256	0.9987861
5		House	256 x 256	0.9996471
6		Trees	256 x 256	0.9996436

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

$$PSNR = 10\,log_{10}\left(\frac{max^2}{MSE}\right) \tag{7}$$

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.

$$MSE = \frac{1}{mxn}\sum_{x=1}^{m}\sum_{y=1}^{n}\left(D(x,y)-S(x,y)\right)^2 \tag{8}$$

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:

$$SSIM\,(D,S) = \frac{(2\mu_x\mu_y + P_1)\,(2\sigma_{xy} + P_2)}{\left(\mu_x^2+\mu_y^2+P_1\right)\,\left(\sigma_x^2+\sigma_y^2+P_2\right)} \tag{9}$$

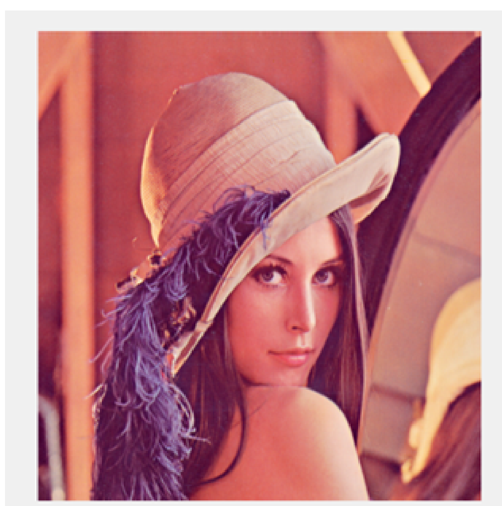

Fig 4. Plain lenna Image 512X512

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

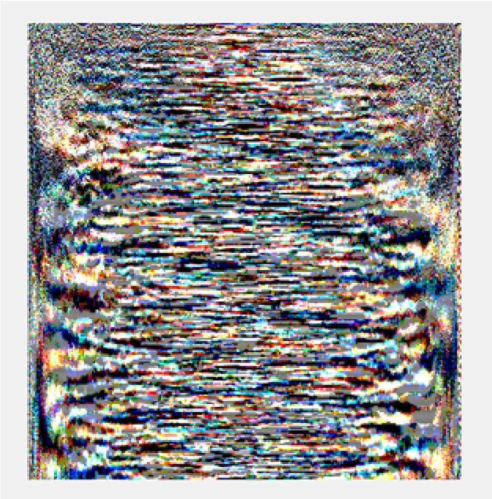

Fig 5. Encrypted lenna Image

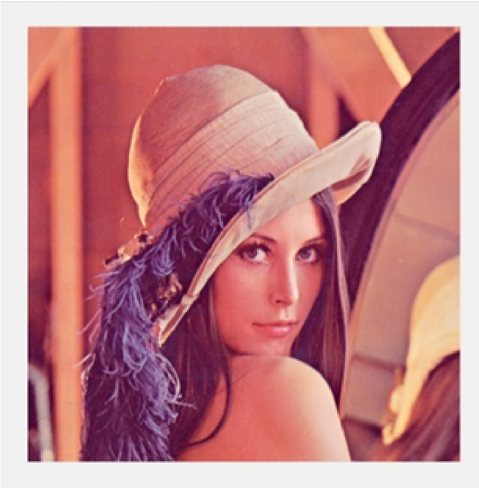

Fig 6. Decrypted lenna Image

Fig 7. Plain Baboon Image

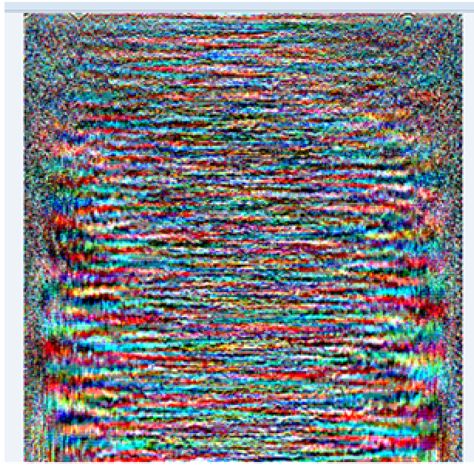

Fig 8. Encrypted Baboon Image

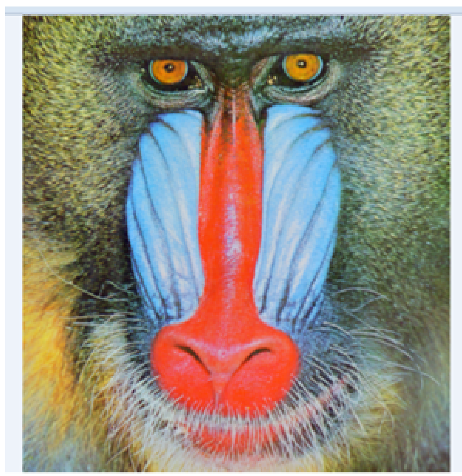

Fig 9. Decrypted Baboon Image

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

		Proposed Method	**DLSS**	Valandar, M. Y., et. Al [9].		Jassim FA [13]		Gutub AA-A et. al. [14]		Muhammad K., et.al. [15]	
#	Image	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM
1	F16	**60.1274**	**0.9999**	53.7294	0.9999	40.2347	0.9797	45.6879	0.9964	47.4902	0.9985
2	Baboon	**61.0083**	**0.9999**	48.5478	0.9998	39.9997	0.9925	46.5568	0.9985	48.9536	0.9992
3	House	**60.2182**	**0.9999**	53.2479	0.9997	40.2518	0.9860	47.6956	0.9974	51.1564	0.9989
4	Trees	**67.3691**	**0.9999**	49.8697	0.9998	39.5397	0.9858	38.2702	0.9956	38.5421	0.9970

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 4. Comparison of PSNR , SSIM and MSE values

#	Plain Image	Image Size	PSNR	SSIM	MSE
1	Lenna	512 x 512	59.54302	0.999965	0.07224
2	Lenna	256 x 256	60.14874	0.999980	0.01873
3	F16	256 x 256	60.12744	0.999940	0.01768
4	Baboon	256 x 256	61.00826	0.999975	0.01379
5	House	256 x 256	60.21819	0.999952	0.01843
6	Trees	256 x 256	67.36909	0.999990	0.00175

shows the effective hiding of cipher data in the audio signal. PSNR values >=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.

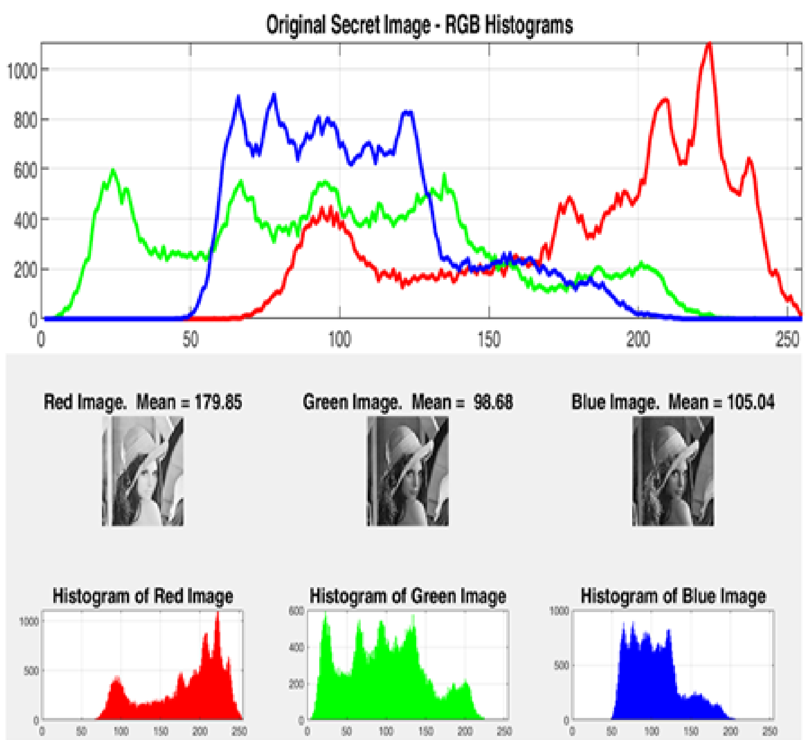

Fig 10. RGB Histogram of Secret Image

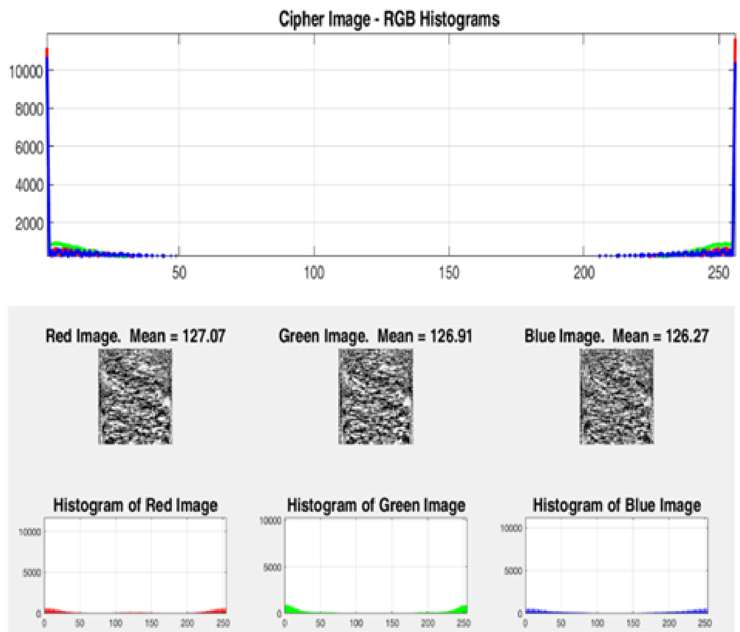

Fig 11. RGB Histogram of Cipher Image

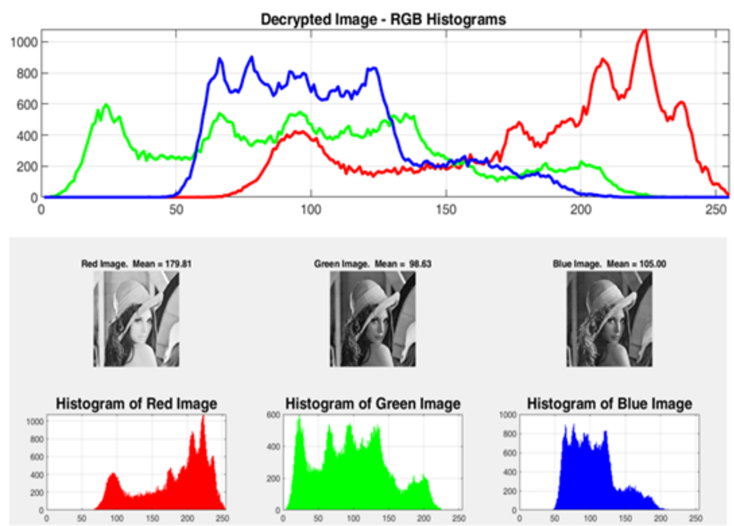

Fig 12. RGB Histogram of Decrypted Image

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

1) Khan M, Waseem HM. A novel image encryption scheme based on quantum dynamical spinning and rotations. *PLOS ONE*. 2018;13(11):e0206460. Available from: https://doi.org/10.1371/journal.pone.0206460.
2) Yang B, Liao X. A new color image encryption scheme based on logistic map over the finite field ZN. *Multimedia Tools and Applications*. 2018;77(16):21803–21821. Available from: https://doi.org/10.1007/s11042-017-5590-0.
3) Teng L, Wang X, Meng J. A chaotic color image encryption using integrated bit-level permutation. *Multimedia Tools and Applications*. 2018;77(6):6883–6896. Available from: https://doi.org/10.1007/s11042-017-4605-1.
4) Sneha PS, Sankar S, Kumar AS. A chaotic colour image encryption scheme combining Walsh–Hadamard transform and Arnold–Tent maps. *Journal of Ambient Intelligence and Humanized Computing*. 2020;11(3):1289–1308. Available from: https://doi.org/10.1007/s12652-019-01385-0.
5) Broumandnia A. The 3D modular chaotic map to digital color image encryption. *Future Generation Computer Systems*. 2019;99:489–499. Available from: https://doi.org/10.1016/j.future.2019.04.005.
6) Alexan W, Elbeltagy M, Aboshousha A. RGB Image Encryption through Cellular Automata, S-Box and the Lorenz System. *Symmetry*. 2022;14(3):443. Available from: https://doi.org/10.3390/sym14030443.
7) Al-Roithy BO, Gutub A. Remodeling randomness prioritization to boost-up security of RGB image encryption. *Multimedia Tools and Applications*. 2021;80(18):28521. Available from: https://doi.org/10.1007/s11042-021-11051-3.
8) Shaji C, Sam IS. A new data encoding based on maximum to minimum histogram in reversible data hiding. *The Imaging Science Journal*. 2019;67(4):202–214. Available from: https://doi.org/10.1080/13682199.2019.1592892.
9) Valandar MY, Barani MJ, Ayubi P, Aghazadeh M. An integer wavelet transform image steganography method based on 3D sine chaotic map. *Multimedia Tools and Applications*. 2019;78(8):9971–9989. Available from: https://doi.org/10.1007/s11042-018-6584-2.
10) Ayub N, Selwal A. An improved image steganography technique using edge based data hiding in DCT domain. *Journal of Interdisciplinary Mathematics*. 2020;23(2):357–366. Available from: https://doi.org/10.1080/09720502.2020.1731949.
11) Kaur R, Singh B. A hybrid algorithm for robust image steganography. 2021. Available from: https://doi.org/10.1007/s11045-020-00725-0.
12) Singh H. Color Image Steganography Techniques - A Review. *RA Journal of Applied Research*. 2018. Available from: https://doi.org/10.18535/rajar/v4i1.01.
13) Jassim FA. A novel steganography algorithm for hiding text in image using five modulus method. 2013. Available from: https://arxiv.org/ftp/arxiv/papers/1307/1307.0642.pdf#:~:text=The%20novel%20algorithm%20is%20called,a%20non%2Dmultiples%20of%205.
14) Gutub A. Pixel Indicator Technique for RGB Image Steganography. *Journal of Emerging Technologies in Web Intelligence*. 2010;2(1). Available from: https://doi.org/10.4304/jetwi.2.1.56-64.
15) Muhammad K, Jamil A, Sajjad M, Zubair M. Secure Image Steganography using Cryptography and Image Transposition. *NED University Journal of Research*. 2015;12:81–91. Available from: https://doi.org/10.48550/arXiv.1510.04413.
16) Mehra I, Fatima A, Nishchal NK. Gyrator wavelet transform. *IET Image Processing*. 2018;12(3):432–437. Available from: https://doi.org/10.1049/iet-ipr.2017.0666.
17) Atta R, Ghanbari M. A high payload data hiding scheme based on dual tree complex wavelet transform. *Optik*. 2021;226:165786. Available from: https://doi.org/10.1016/j.ijleo.2020.165786.
18) Chithra PL, Tamilmathi AC. 3D LiDAR point cloud image codec based on Tensor. *The Imaging Science Journal*. 2020;68(1):1–10. Available from: https://doi.org/10.1080/13682199.2020.1719747.
19) Chithra PL, Aparna R. Voice Signal Encryption Scheme Using Transformation and Embedding Techniques for Enhanced Security. *2018 2nd International Conference on Imaging, Signal Processing and Communication (ICISPC)*. 2018;p. 149–154. Available from: https://doi.org/10.1109/ICISPC44900.2018.9006681.
20) Sabeti V, Amerehei M. Secure and Imperceptible Image Steganography in Discrete Wavelet Transform Using the XOR Logical Function and Genetic Algorithm. *The ISC International Journal of Information Security*. 2022. Available from: https://doi.org/10.22042/isecure.2022.274305.641.
21) Sharma H, Mishra DC, Sharma RK, Kumar N. Multi-image steganography and authentication using crypto-stego techniques. *Multimedia Tools and Applications*. 2021;80(19):29067–29093. Available from: https://doi.org/10.1007/s11042-021-11068-8.
22) Jan A, Parah SA, Hussan M, Malik BA. Double layer security using crypto-stego techniques: a comprehensive review. *Health and Technology*. 2022;12(1):9–31. Available from: https://doi.org/10.1007/s12553-021-00602-1.