REVAMPING HYPERSPECTRAL IMAGE SECURITY WITH LAB COLOR SPACE ENCRYPTION

1st Neelavathy Pari S
Assistant Professor, Department of Computer Technology,
Anna University, MIT Campus
Chennai, India
neela_pari@yahoo.com

2nd Ramyaa P
Department of Computer Technology
Anna University, MIT Campus
Chennai, India
ramyaaprasath13@gmail.com

3rd Priyadharshini R
Department of Computer Technology
Anna University, MIT Campus
Chennai, India
priyadarshini01.r@gmail.com

4th Pramoth G
Department of Computer Technology
Anna University, MIT Campus
Chennai, India
pramoth7773@gmail.com

***Abstract*—Hyperspectral imaging is a remote sensing technology that captures and analyzes the spectrum of light reflecting off an object, providing a wealth of information about its chemical and physical properties. However, it's frequently necessary to prevent unauthorized access to the delicate information that one's hyperspectral photographs contain. In order to protect one's hyperspectral data, encryption is used. In many industries, including remote sensing, medical imaging, and military, hyperspectral imaging has become a strong technique that is widely used. Nevertheless, there are growing worries about hyperspectral images' security during transmission and storage as a result of their expanding use. Encryption techniques have been used to lessen the hazards connected to hyperspectral picture security. However, there are some drawbacks to the encryption techniques now in use, including security gaps, efficiency issues, and attack susceptibility. However, this method comes with a number of drawbacks, including higher computational complexity, decreased image quality, difficult key management, compatibility concerns, and decreased performance. The proposed method has successfully addressed these drawbacks and demonstrated significant improvements in terms of security, efficiency, and robustness. In fact, the results of the proposed work have been highly promising, with a close proximity of 97% to the desired security standards.**

***Index Terms*—CIELAB, HSV, image Processing, Chaotic Encryption**

I. Introduction

Hyperspectral imaging is a technique that enables the acquisition of spectral data from an object or a scene. It produces a high spectral resolution by capturing small spectral bands that are evenly spaced across the electromagnetic spectrum. Various sectors, including remote sensing, medical imaging, and agriculture, use hyperspectral imaging extensively. The material composition, physical characteristics, and state of the object or scene are all revealed in the spectrum data collected by hyperspectral imaging. This data can be used to discover anomalies, categorize items, and extract helpful features. Due to recent developments in sensor technology, image processing methods, and computing capacity, hyperspectral imaging has become increasingly popular. However, there are substantial difficulties in storing, processing, and analyzing hyperspectral data due to its enormous dimensionality. As a result, plenty of methods have been developed to decrease the dimensionality of hyperspectral data while preserving the important information. These methods include spectrum unmixing, dimensionality reduction, and feature extraction. The development of these methods has made it easier to apply hyperspectral imaging in practical settings and created new possibilities for research and advances in technology. However, it's frequently necessary to prevent unauthorised access to the delicate information that one's hyperspectral photographs contain. In order to protect one's hyperspectral data, encryption is used. In encrypting and decrypting data, chaotic encryption employs chaotic systems to produce random and unpredictable keys. In order to make an image unreadable to unauthorized users, the pixel values of an image are scrambled using chaotic encryption techniques. A solution for picture security that has received a lot of attention recently is chaotic encryption. However, the quality of the chaotic system employed and the encryption method used determine the efficacy and security of chaotic encryption in images.

Consequently, a number of methods have been put forth to increase the effectiveness and security of chaotic encryption in images, including the use of hybrid encryption schemes, the optimisation of the chaotic system parameters, and the application of permutation and diffusion processes.

Despite its potential advantages, chaotic encryption in images is still a relatively young field of study, and further research is required to fully explore its capabilities. The application's performance limits and security needs must also be carefully taken into account when implementing chaotic

encryption techniques. Chaotic encryption has the potential to play a significant role in the development of safe and reliable communication and storage systems, which is projected to be a result of the rise of digital data and the rising demand for data security. However, this method comes with a number of drawbacks, including higher computational complexity, decreased image quality, difficult key management, compatibility concerns, and decreased performance

II. Problem Statement

Hyperspectral imaging technology has become an indispensable tool in various industries such as agriculture, mineral exploration, and environmental monitoring. However, it's frequently necessary to prevent unauthorised access to the delicate information that hyperspectral photographs contain. Although encryption is a popular method for protecting hyperspectral data, it also comes with a number of difficulties. The original hyperspectral data may change during the encryption process, reducing the quality of the image and changing how it can be analysed. Usually encryption converts hyperspectral images only to RGB color space. Secure key management is necessary for the usage of encryption as well, and this process can be difficult and time-consuming. Additionally, not all image processing tools may be compatible with encrypted hyperspectral pictures, restricting their usability in some applications.

III. Literature Survey

A. Comparison Of CIELAB Color Space

To separate the colour and brightness information in a picture, a linear transformation in the CIELAB colour space is introduced in [4]. The technique first converts the image to CIELAB, then returns it to RGB for additional processing after using a linear adjustment to increase brightness in the L channel. It is limited to linear transformations in CIELAB and works well for simple colour distributions but may struggle with complex colour distributions. The method's applicability is determined by the qualities of the image. HSV or Lab colour space is preferred for hydroponic monitoring, with HSV being useful for recording hue and saturation data.

The authors of [11] identified which color space is suitable for the application by processing the pictures using both color spaces to extract color information and then evaluate the accuracy of each color space in detecting nutrient deficiencies in hydroponic plants. A drawback is that this paper only compares both the color spaces in the context of hydroponic monitoring. They have also not considered other color spaces such as RGB.

The performance of each color space was evaluated using three different classification methods: k-nearest neighbours, support vector machines, and random forests. The results showed that CIELAB and CIELUV outperformed RGB and HSV in all classification methods. Additionally, the study found that the choice of classification method had a greater impact on classification performance than the choice of color space. Overall, [2] suggests that using CIELAB or CIELUV color spaces can improve the accuracy of material classification in images. The paper further notes that future research could explore the use of other color spaces or combine multiple color spaces to further improve classification performance. A limitation here is that they used a dataset of only 10 different materials, which may not be representative of the full range of materials that could be encountered in real-world applications.

When photographing natural scenery and artwork, Linhare et al. in [8] compared the colour fidelity of RGB cameras and hyperspectral imaging. They discovered that RGB cameras have a fair amount of difficulty catching the complete spectrum of colours in paintings, especially subtle fluctuations and colours in shadows and highlights. According to the study, hyperspectral imaging may be more capable of catching colours with more accuracy. It should be emphasised that a specific kind of RGB camera and hyperspectral imaging system were employed in the investigation.

B. About Encryption Algorithms

A new chaotic image encryption technique based on the spiral-transform-based fractal sorting matrix (STFSM) is proposed in a study by Y. Xian et al. in [17]. The STFSM is an infinitely scalable fractal sorting matrix with disorder, self-similarity, and iterability. STFSM serves as the main encryption and decryption algorithm in the suggested strategy. The average information entropy of encrypted images using the method is not as close to the theoretical value as other methods, according to experimental results.

By testing the suggested chaotic encryption method [18] for bifurcation graphs, Lyapunov exponents, and Shannon entropy, it is demonstrated that it is resistant to dynamic degradation and exhibits unpredictability and chaos. It features a larger chaotic space, which increases the selectivity of key system parameters. The method takes a while to iterate, and it might not be able to withstand common cracks.

The system is made up of four basic parts: key generation, content selection, encryption, and decryption. The content selection module chooses the image material that will be encrypted using a chaos-based random number generator. The key generation module is in charge of producing encryption and decryption keys based on LS chaotic maps, which are employed in the encryption and decryption modules to generate encryption keys. The system's confusing target detection boundary determination, which could lead to weak encryption of crucial image features, is a negative. [6]

In [15] Yang, Z et al propose a system which first performs a gyrator transformation on the hyperspectral image to transform it from spatial domain into frequency domain. This gyrator transformed hyperspectral image in the frequency domain is then encrypted using a triangular association encryption algorithm. The encrypted image is then signed using a digital signature to ensure the authenticity and integrity of the image. One of the major limitations is the requirement of significant computational resources depending on the size and complexity.

The encryption technique in [5] combines a phase-truncated discrete multiple-parameter fractional Fourier transform with

an enhanced binary tree structure for hyperspectral picture encryption. To demonstrate its performance, it provides technical information and results from numerical simulations. It is challenging to assess the results' validity and their applicability to various hyperspectral datasets without access to the simulation's specifics. The study doesn't address some of the flaws and vulnerabilities in the suggested algorithm.

A nonlinear image encryption method based on multivariate polynomials is put forward in [3]. Confusion and diffusion are the two phases of the encryption scheme. Diffusion is accomplished through a series of iterations using multivariate polynomials, whereas confusion is accomplished by arbitrarily choosing permutation functions and applying them to the image pixels. A number of experiments are used to evaluate the proposed method, and the findings indicate that it is successful in terms of security and computational effectiveness.

A novel encryption algorithm based on a multistage chaos system and DNA encoding was proposed by Li et al. in 2021. The algorithm encrypted the image by employing multiple chaotic systems at various stages, and it was made more secure by using the DNA encoding technique. The experimental findings demonstrated the proposed algorithm's high security and effective encryption. [7]

Liu, J., & Liu, Y present a new image encryption scheme based on hyper-chaotic system and dynamic state variables. To increase the security of image encryption, the proposed scheme combines the benefits of the hyper-chaotic system and dynamic state variables. Dynamic state variable diffusion and hyper-chaotic scrambling are the two stages of the encryption process. The proposed scheme in [9] is effective, secure, and resistant to common attacks, according to experimental findings.

An image encryption technique based on DNA encoding and spatiotemporal chaos is presented in the study by Song and Qiao [12]. The algorithm consists of three steps: converting the image to a DNA sequence, subjecting it to spatiotemporal chaos, and encrypting the image. The approach provides a novel combination of DNA encoding and spatiotemporal chaos to address the issue of image encryption.

The suggested approach in [13] generates encryption keys from a hyper-chaotic system with positive Lyapunov exponents. There are two steps to it: permutation and dissemination. While the permutation stage is based on a chaotic permutation scheme, the diffusion stage uses a hyper-chaotic substitution scheme. Numerous tests have shown that the method is very secure and resilient against different forms of attacks, including statistical attacks. Through thorough experimentation, the algorithm's robustness and effectiveness were proven, proving its capacity to offer excellent security and withstand many attack scenarios.

The image encryption method utilizing a 3D Henon map and discrete wavelet transform in [14] is composed of two stages. In the first stage, the plaintext image is split into non-overlapping blocks, and the pixels inside each block are randomly shuffled using a 3D Henon map. To add more security, the shuffled blocks are further processed in the second stage using a discrete wavelet transform and a permutation operation. The experimental findings demonstrated that the suggested scheme attained a high level of efficiency and security.

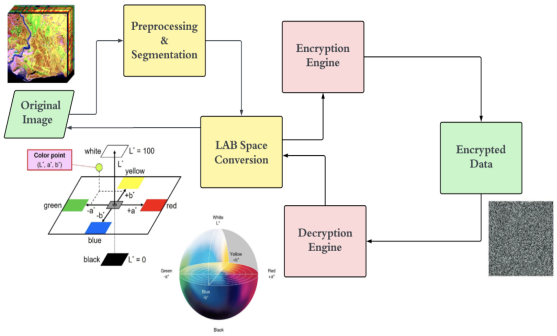

Fig. 1. LAB Encryption Architecture

Using a chaotic function switching mechanism, a unique image encryption technique is presented in [16]. A 1D byte sequence is used for confusion and diffusion together with three chaotic maps in the symmetric cypher. The chaotic maps arrange scrambled image bytes to choose between decrypted and unencrypted bytes, while a third map introduces a stochastic value via an exclusive-or operation to increase the security and encryption capabilities of the technique.

A unique image encryption technique using a chaotic function switching mechanism is proposed in [16]. Three chaotic maps and a 1D byte sequence are used in the symmetric cypher to create confusion and diffusion. In order to improve the security and encryption capabilities of the algorithm, a third map injects stochastic values via an exclusive-or operation. Scrambled image bytes are sorted using the chaotic maps, choosing among decrypted and unencrypted bytes.

IV. Implementation

This study suggests an improved encryption method for LAB colour hyper spectral images. In order to balance security and image data loss, it assesses different encryption techniques based on computational complexity, image quality, and overall performance. A trustworthy and effective encryption technique is suggested after evaluating the shortcomings of earlier methods, and it is created specifically for hyper spectral images in the LAB colour space. Because LAB colour space represents information in a perceptually consistent manner that is in line with human vision, its importance is emphasised. The performance of the suggested algorithm is thoroughly assessed and contrasted with existing encryption methods in an effort to safely save hyper spectral images while maintaining their worth. The results of this study will have a substantial impact on secure storage solutions for hyper spectral imaging and will serve as a road map for future advancements in secure storage technologies. The architecture as shown is made up of four parts. **Module 1**: Hyperspectral Images Preprocessing

- The hyperspectral image dataset used for encryption is contained in this component. Google Cloud Storage is where the dataset is kept. This data is essential for image preprocessing.
- Various preprocessing techniques are applied. Image segmentation such as edge detection techniques, line detection are used.

Module 2: Component for L*a*b Color Space Conversion

- The hyperspectral image is first converted from its initial form to the L*a*b color space by using components.
- This conversion helps minimise the dimensionality of the image and improves the encryption algorithm's performance.

Module 3: Engine for Encryption

- The encryption algorithm for encrypting the hyperspectral images is contained in this component.
- The encryption algorithm works by transforming the Lab color space image into a format that is resistant to attack.
- This transformation ensures that the hyperspectral image data remains secure during transmission and storage.

Module 4: Engine for Decryption

- The decryption algorithm is the counterpart of the encryption algorithm and is responsible for transforming the encrypted hyperspectral image data back to its original form.
- The decryption algorithm performs the reverse transformation of the encryption algorithm, recovering the original Lab color space image from the encrypted format.
- The decryption algorithm applies a decryption key that corresponds to the encryption key used during the encryption process.
- The decryption algorithm ensures that the original data is protected during transmission and storage and can only be accessed by authorised users with the correct decryption key.

A. About The Dataset

A hyperspectral picture dataset of Indian pines was employed. The dataset was gathered over farmland in Indiana, USA, by the Airborne Visible/Infrared Imaging Spectrometer (AVIRIS) sensor. The dataset is frequently used in remote sensing and machine learning research to test and develop hyperspectral image processing techniques and models.

The dataset has a spatial resolution of 20 meters per pixel and 224 spectral bands, each of which corresponds to a different light wavelength between 0.4 and 2.5 microns. The dataset has undergone preprocessing to improve the quality and remove atmospheric influences . There are 21,025 data points in the preprocessed dataset, each measuring 145x145 pixels. The spectral signature of each pixel in the dataset containing the materials and objects in the image, corresponds to a specific spot on the ground.

B. Preprocessing

As part of the preprocessing stage for the Indian Pines hyperspectral dataset, the dataset was reshaped into a two-dimensional array of (samples, features), and Principal Component Analysis (PCA) was used to reduce its dimensionality to 30 components.

The PCA-transformed data was subsequently normalized to have values between 0 and 1, after which it was reshaped into the three-dimensional array of the original data. To demonstrate the essential components of the PCA decomposition, the top three eigenvectors are displayed as shown. Each

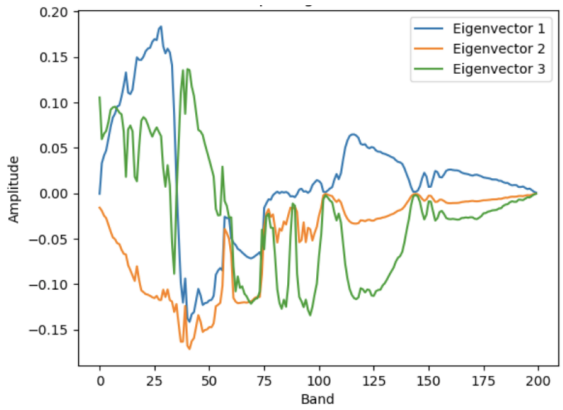

Fig. 2. Eigenvectors

eigenvector is shown as a line in the resulting plot, with the band number on the x-axis and the amplitude of the eigenvector at that band on the y-axis. Using the ndimage package from Scipy, a Gaussian filter is applied to each band of a hyperspectral data cube. Gaussian filters are a type of low-pass filter that smoothen images by removing high-frequency noise and gently blurring the image. In order to remove noise from the image, filtering is a crucial pre-processing step in image processing, particularly in hyperspectral imaging. The ability of Gaussian filtering to eliminate noise without impairing the sharpness of the image's edges makes it a widely utilized technique in image processing. In the PCIS (Principal

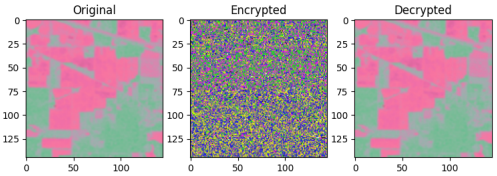

Fig. 3. Spectral Smoothing using Gaussian filter

Component-based Image Encryption System) encryption approach, the integration of a Gaussian filter, shown in Figure 3.3, is very important, particularly in reducing noise present in the hyperspectral image. The chaotic encryption algorithm's use of random number generation could be disrupted by interference, however the Gaussian filter mitigates this risk by lowering noise, simplifying the encryption procedure overall.

The quality and clarity of the hyperspectral image are significantly improved by the use of a Gaussian filter, which in turn makes feature extraction and representation more efficient.

Due to its capacity to lower noise and improve image smoothness, Gaussian filtering is frequently used in the preprocessing step of hyperspectral images. In order to maximize the image quality, which directly affects the precision and dependability of following encryption processes, this preprocessing step is crucial.

C. LAB Color Space Conversion

1) Conversion to CIELAB color space: The image is initially converted from the RGB color space to the LAB color space. The chaotic permutation matrix can now be applied independently to the image's three different color channels (L, a, and b), as shown, which is a crucial step in the PCIS encryption process.The device-independent LAB color space was created to closely replicate human vision. The image's brightness is represented by the L channel, while its chrominance is represented by the a and b channels. This increases the strength of the algorithm by allowing us to apply various chaotic maps to the L, a, and b channels. PCIS encryption starts a separate pseudorandom number generator for each color channel after converting the image to the LAB color space. A chaotic permutation matrix is simultaneously created using a nonlinear function. These elements are essential to the encryption procedure. After reconstruction, the image is

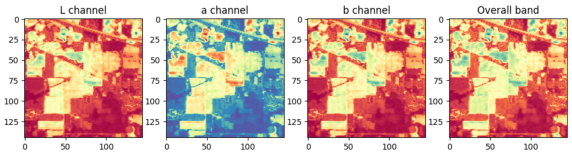

Fig. 4. A single band and its corresponding L, a, b channels

delivered as an encrypted image along with the encryption keys. Overall, the Pseudorandom Chaotic Image Scrambling (PCIS) encryption technique is now more secure and robust thanks to the conversion to the LAB color space.

2) Encryption Engine: The encryption algorithm proposed is Pseudorandom Chaotic Image Scrambling. The input for the algorithm is the image to be encrypted and seed values which is a list of 3 pseudorandom number generator keys for each color channel in LAB color space. The image given as input is first converted to LAB color space. Using the seed, the pseudorandom number generator for each color channel is initialized.

For each color channel, a chaotic permutation matrix is created by initializing three variables as numpy arrays of zeros with the same shape as the first two dimensions of the LAB space image. Then, for five iterations, update the permutation matrices perm using Equation (i),

$$\text{perm} = (\text{perm}^{\alpha} + i)\%256 \tag{i}$$

where α is in a range of 2 to 3. In Equation (3.1), i represents the loop variable and perm represents the permutation matrix.

Algorithm 1: pcis_encrypt_lab Algorithm

Input: img: Input image in BGR color space,
seed: Seed for pseudorandom number generator
Output: img_scrambled: Encrypted image in LAB color space,
seed: The same seed used for encryption
Function *pcis_encrypt_lab(img, seed)*:
  Data: img, seed
  Result: img_scrambled, seed
  img_lab ← `cv2.cvtColor` (img, cv2.COLOR_BGR2LAB);
  rng_l ← [`np.random.default_rng` (key) **for** key **in** seed];
  perm_l ← [np.zeros_like(img_lab[:,:,0]) **for** i **in** range(3)];
  for *i **in** range(5)* **do**
    perm_l ← `np.mod` (`np.power` (perm_l, 2.1) + i, 255);
  end
  perm_l ← perm_l.`ravel` ().`argsort` ().`reshape` (perm_l.shape);
  mask_l ← rng_l.integers(0, 256, size=img_lab.shape[:2], dtype=np.uint8);
  img_scrambled ← cv2.merge([cv2.bitwise_xor(img_lab[:,:,0], mask_l),]);
  img_scrambled[:,:,0] ← np.take(img_scrambled[:,:,0], perm_l.`ravel` ()).`reshape` (img_lab[:,:,0].shape);
  return *img_scrambled, seed*;

Reshape the permutation matrices into 1D arrays, sort them, and reshape them back into 2D matrices with the same shape as the permutation matrices and store the resultant matrices. PIC's encryption has several benefits, including a high level of security, resistance to different assaults, robustness, and post-quantum security. Generate a random mask for each color channel using the corresponding Pseudorandom number generator. Next, scramble the image using the masks and permutation matrix. Finally, return the scrambled image and the three random number generators as output.

3) Decryption Engine: The encrypted image and a seed value are inputs to the decryption engine. The engine initializes three pseudorandom number generators using the seed value. The decryption procedure depends on these generators. Three permutation matrices are produced by applying the chaotic map defined by Equation (i) to a zero matrix to begin the decryption procedure. The encrypted image must be decrypted using these permutation matrices. These masks are modified to take into account the input image's dimensions, which are scrambled. Then reshape the permutation matrix then reordering the corresponding color channel, and finally reshaping it back to the original shape.

Algorithm 2: pcis_decrypt_lab Algorithm

Input: img_scrambled: Encrypted image in LAB color space,
seed: Seed used for encryption
Output: img_bgr: Decrypted image in BGR color space
Function *pcis_decrypt_lab(img_scrambled, seed)*:
  Data: img_scrambled, seed
  Result: img_bgr
  rng_l← [`np.random.default_rng` (key) **for** key **in** seed];
  perm_l← [np.zeros_like(img_scrambled[:,:,0]) **for** i **in** range(3)];
  for *i **in** range(5)* **do**
    perm_l ← `np.mod` (`np.power` (perm_l, 2.1) + i, 255);
  end
  perm_l ← perm_l.`ravel` ().`argsort` ().`reshape` (perm_l.shape);
  mask_l ← rng_l.integers(0, 256, size=img_scrambled.shape[:2], dtype=np.uint8);
  mask_l ← `np.broadcast_to` (mask_l[..., None], img_scrambled.shape);
  img_permuted ← `cv2.merge` ([`np.take` (img_scrambled[:,:,0], perm_l.`ravel` ().`argsort` ()).`reshape` (img_scrambled[:,:,0].shape), `np.take` (img_scrambled[:,:,1]);
  img_permuted[:,:,0] ← `np.bitwise_xor` (img_permuted[:,:,0], mask_l[:,:,0]);
  img_bgr ← `cv2.cvtColor` (img_permuted, cv2.COLOR_LAB2BGR);
  return *img_bgr*;

V. Results and Discussion

The performance of the proposed method across multiple spectral bands can be thoroughly assessed by comparing the original and encrypted images. The suggested approach works well for the entire range of spectral bands in the hyperspectral image by making sure that the encryption and subsequent decryption process accurately restore the original image. This verification is necessary to determine whether the algorithm is appropriate for use in practical applications. The suggested encryption method offers a solid solution that can be securely used in real-world applications by successfully proving the precise restoration of the original hyperspectral image across all spectral bands. This verification strengthens the algorithm's performance and confirms its applicability for secure hyperspectral picture transmission, storage, and processing, enhancing their dependability and confidentiality across a range of fields.

A. Visualization Of Algorithm Outputs

The evaluation of an encryption algorithm's efficiency and functionality relies heavily on the visualization of algorithm results. Figures below provide encryption and decryption results for various bands in the hyperspectral image within the context of the study, demonstrating the algorithm's performance for various spectral bands. The original image

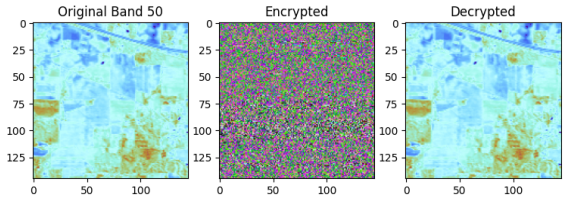

Fig. 5. Original, Encrypted and Decrypted images of Band 50

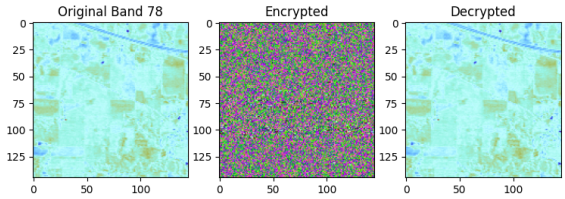

Fig. 6. Original, Encrypted and Decrypted images of Band 78

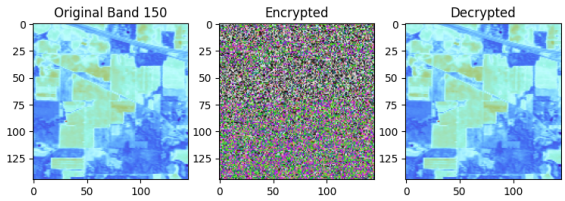

Fig. 7. Original, Encrypted and Decrypted images of Band 150

corresponds to the unencrypted hyperspectral image with all of its spectral bands kept in their original configuration. The exact content and spectral features of the original hyperspectral data are reflected in this image, which serves as a baseline reference. The decrypted image is the result of applying decryption techniques to the encrypted image, thereby recovering the original hyperspectral image with all its spectral bands restored. Comparing the original, encrypted, and decrypted images of various bands can help evaluate the effectiveness of the encryption and decryption techniques.It is important to note that the quality of the decrypted image may depend on the strength of the encryption algorithm used. It is important to note that the quality of the decrypted image may depend on the strength of the encryption algorithm used.

B. Testing

1) Performance Metrics: Three picture quality metrics—Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index (SSIM), and Mean Squared Error (MSE)—are calculated for this technique. These measurements are crucial for assessing how well picture encryption and decryption techniques perform.

The PSNR measures the ratio of the maximum possible power of the signal to the power of the noise, and is expressed in decibels (dB). The higher the PSNR value, the better the quality of the decrypted image. The SSIM compares the structural similarity between the original and decrypted images, and ranges between -1 and 1, where 1 indicates similarity. Perfect similarity means the original image and the decrypted image are very close in similarity.

A metric for measuring the average squared difference between the original image and the encrypted image is the Mean Squared Error (MSE). Because it represents a closer likeness to the original image, a lower MSE value denotes a higher quality outcome. The decryption algorithm was specifically evaluated, and the results show that the algorithm worked well in terms of image quality. The acquired MSE scores are higher than the reference scores. The higher MSE scores imply that there are few differences between the decrypted and original images, which closely match each other. This suggests that the decryption algorithm successfully recovered the image to its original state while satisfactorily maintaining its quality.

The expected values for PSNR and SSIM should be high for a solid image encryption technique, while the expected value for MSE should be low as shown in Table 5.1. In general, good image quality and a high degree of resemblance between the original and encrypted images are indicated by a PSNR value larger than 30 dB, an SSIM value greater than 0.9, and an MSE value less than 0.01. However, depending on the specific application and the required level of image quality, the ideal values for these parameters may change.

Metric	Recommended score	Proposed algorithm's score	Difference
PSNR	40	49.9242	-9.9242
SSIM	1	0.9998	0.0002
MSE	0	0.6616	-0.6616

Fig. 8. Obtained metric values in comparison with expected values

The predicted values for these metrics vary depending on the encryption method chosen. Because they enable a complete reconstruction of the original image without causing any data loss, lossless encryption algorithms frequently produce higher PSNR values. For lossless encryption, PSNR values above 60 dB are regarded as great, but values over 40 dB are still considered to be good. Lossy encryption methods, on the other hand, produce lower PSNR values because data is inevitably lost during the encryption process. A PSNR value between 20 and 40 dB is regarded as good for lossy encryption, with higher values denoting higher quality. However, in order to gain a thorough evaluation of image quality, it's crucial to take into account additional metrics like SSIM and MSE.

2) Histogram Analysis: The distribution of an image's pixel values is visualized using a histogram plot, which reveals an image's susceptibility to statistical attacks. For an encrypted image to withstand statistical attacks, a flatter, more uniform histogram is preferable.

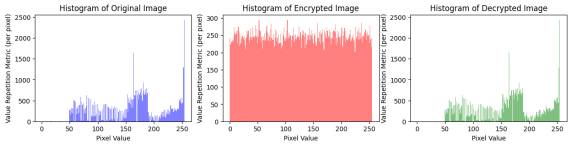

Fig. 9. Histogram analysis of original, encrypted and decrypted hyperspectral image

The blue histogram of the original image reveals that the bulk of pixel values are in the range of 50 to 250, with a sharp drop in values at around 200, indicating that the general tone of the image is darker. The histogram of the encrypted image,i.e red histogram, needs to be consistent enough to withstand statistical attacks; otherwise, attackers could use the histogram of the encrypted image to extract meaningful information about the original image.The histogram of the encrypted image is a fairly uniform distribution.The green histogram of the decrypted image as shown in Fig has a comparable distribution of pixel values to the original image histogram, proving that the encryption and decryption processes did not materially change the distribution of pixel values in the image. This implies that the encrypted image keeps the original image's general visual qualities. The well-known Lena image, which

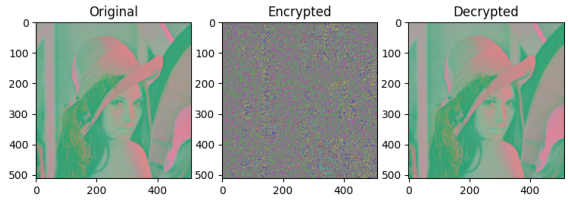

Fig. 10. Original, Encrypted and Decrypted images of Lena

serves as a standard reference for many image preprocessing research, is the original image utilized as a baseline. The pixel intensities of this image show a distribution dispersed across a wide range of values, with a peak seen around the mid-range values. This distribution shows that there is a variety of visual information in the Lena image, including both darker and brighter parts. The distributions of the decrypted image and the

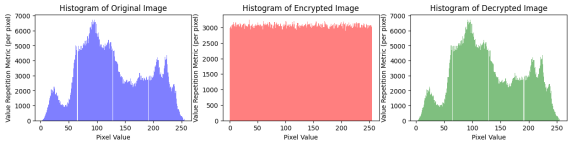

Fig. 11. Histogram comparison of Lena image

original Lena image are similar, as seen by a comparison of their histograms. This suggests that the decryption procedure was successful in preserving the primary visual aspects of the original image without introducing appreciable modifications or adjustments.

VI. Conclusion

This study proposes an enhanced encryption algorithm for hyperspectral images that have been preprocessed and transformed to LAB color space. The suggested technique addresses the issues raised in the available research and seeks to minimize the trade-off between security and information loss. A novel encryption algorithm that overcomes the flaws of existing strategies by reviewing several encryption methods and evaluating their performance in terms of computational complexity, image quality and overall performance, is offered. Our findings show that the suggested approach is a reliable and efficient way for encrypting hyperspectral images, particularly in LAB color space. In terms of security, complexity and image quality, the approach surpasses current encryption techniques, demonstrating its potential for practical implementation in the safe storage of hyperspectral images. This effort significantly benefits the field of image encryption by introducing a novel encryption technique that can improve security while minimizing data loss. It also discusses the limitations and opportunities of future encryption, as well as the necessity for additional study into the creation of more robust encryption systems.

VII. Future Work

This study shows the potential of utilizing encryption techniques to secure hyperspectral photos and contributes the groundwork for future research in this field. Considering the results, it is expected that this research will drive more research in this field in order to improve the security and accessibility of the systems, increasing the scope for research and industry.

References

[1] T. Adão, J. Hruška, L. Pádua, J. Bessa, E. Peres, R. Morais, and J. J. Sousa (2019) "Hyperspectral Imaging: A Review on UAV-Based Sensors, Data Processing and Applications for Agriculture and Forestry," Journal of Remote Sensing, Vol. 9, No. 11, pp. 1110 - 1140. doi: 10.3390/rs9111110.

[2] R. Bello-Cerezo, F. Bianconi, A. Fernández, E. González, and F. Di Maria (2018) "Experimental comparison of color spaces for material classification," Journal of Imaging, Vol. 4, No. 9, pp. 111-121. doi: 10.3390/jimaging4090111.

[3] B. Yang, H. Deng and L. Huang (2012) "A nonlinear image encryption method based on multivariate polynomials," Optik - International Journal for Light and Electron Optics, Vol. 123, No. 16, pp. 1401-1410, doi: 10.1016/j.ijleo.2011.09.011.

[4] M. F. Hassan (2022) "A uniform illumination image enhancement via linear transformation in CIELAB color space," Multimedia Tools and Applications, Vol. 81, pp. 26331-26343. doi: 10.1007/s11042-022-12429-7.

[5] H. Li, X. Bai, M. Shan, Z. Zhong, L. Liu, and B. Liu (2020) "Optical encryption of hyperspectral images using improved binary tree structure and phase-truncated discrete multiple-parameter fractional Fourier transform," J. Opt., Vol. 22, No. 5, pp. 55403-55412. doi: 10.1088/2040-8986/ab7ae8.

[6] J. Wang, L. Liu, M. Xu, and X. Li (2022) "A novel content-selected image encryption algorithm based on the LS chaotic model," J. King Saud Univ. - Comput. Inf. Sci., Vol. 34, No. 10, pt. A, pp. 8245-8259. doi: 10.1016/j.jksuci.2022.08.007.

[7] Y. Li, H. Jiang, and Y. Zhou (2021)"A Novel Image Encryption Algorithm Based on Multistage Chaos System and DNA Encoding," J. Comput. Theor. Nanosci., Vol. 18, No. 12, pp. 7655-7663. doi: 10.1166/jctn.2021.10913.

[8] J. M. M. Linhares, J. A. R. Monteiro, A. Bailão, L. Cardeira, T. Kondo, S. Nakauchi, M. Picollo, and J. C. Neves (2019) "How good are RGB cameras retrieving colors of natural scenes and paintings?—A study based on hyperspectral imaging," Color Res. Appl., Vol. 44, No. 4, pp. 598-610. doi: 10.1002/col.22398.

[9] J. Liu and Y. Liu (2016) "An image encryption scheme based on hyper-chaotic system and dynamic state variables," Multimed. Tools Appl., Vol. 75, No. 16, pp. 9915-9928. doi: 10.1007/s11042-016-3688-2.

[10] M. J. Khan, H. S. Khan, A. Yousaf, K. Khurshid and A. Abbas (2018) "Modern Trends in Hyperspectral Image Analysis: A Review," in IEEE Access, Vol. 6, pp. 14118-14129, doi: 10.1109/ACCESS.2018.2812999.

[11] T. A. Setyawan, S. A. Riwinanto, Helmy, A. Nursyahid, and A. S. Nugroho (2018), "Comparison of HSV and LAB Color Spaces for Hydroponic Monitoring System," in 2018 5th International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE), pp. 1-6. doi: 10.1109/icitacee.2018.8576991.

[12] C. Song and Y. Qiao (2015) "A novel image encryption algorithm based on DNA encoding and spatiotemporal chaos," Math. Probl. Eng., Vol. 2015, pp. 1-11. doi: 0.1155/2015/251723.

[13] X. Wang, X. Li, and Y. Li (2013) "A novel image encryption algorithm based on hyper-chaotic system," Opt. Commun., Vol. 291, pp. 242-247. doi: 10.1016/j.optcom.2012.09.041.

[14] L. Yang, Y. Wang, Y. Wei, J. Zhou, X. Wang, and W. Lu (2021) "A secure and high-efficiency image encryption scheme based on 3D Henon map and discrete wavelet transform," Signal Process. Image Commun., Vol. 97, pp. 116225-1162237. doi: 10.1016/j.image.2021.116225.

[15] Z. Yang, Y. Cao, S. Liu, C. Tanougast, W. Blondel, Z. Liu, and H. Chen (2022) "A Novel Signature and Authentication Cryptosystem for Hyperspectral Image by Using Triangular Association Encryption Algorithm in Gyrator Domains," Appl. Sci., Vol. 12, No. 15, pp. 7649-7660. doi: 10.3390/app12157649.

[16] E. Yavuz (2019), "A novel chaotic image encryption algorithm based on content-sensitive dynamic function switching scheme," Opt. Laser Technol., Vol. 114, pp. 224-239, 2019. doi: 10.1016/j.optlastec.2019.01.001.

[17] Y. Xian, X. Wang, X. Wang, Q. Li, and X. Yan (2022), "Spiral-Transform-Based Fractal Sorting Matrix for Chaotic Image Encryption," IEEE Transactions on Circuits and Systems I: Regular Papers, Vol. 69, No. 8, pp. 3320-3327, doi: 10.1109/TCSI.2022.3172116.

[18] X. Wang and P. Liu (2022) "A New Full Chaos Coupled Mapping Lattice and Its Application in Privacy Image Encryption," in IEEE Transactions on Circuits and Systems I: Regular Papers, Vol. 69, No. 3, pp. 1291-1301, doi: 10.1109/TCSI.2021.3133318.

[19] X. Yang, Y. Ye, X. Li, R. Y. K. Lau, X. Zhang and X. Huang (2018), "Hyperspectral Image Classification With Deep Learning Models," in IEEE Transactions on Geoscience and Remote Sensing, Vol. 56, No. 9, pp. 5408-5423, doi: 10.1109/TGRS.2018.2815613.

[20] H. Zhang, H. Chen, H. Zhang, H. Xie, and Y. Li (2021), "A Novel Image Encryption Algorithm Based on Multiple Chaotic Maps and DNA Encoding," IEEE Access, Vol. 9, pp. 90363-90375. doi: 10.1109/ACCESS.2021.3098795.