Conversion of Landsat 8 multispectral data through modified private content-based image retrieval technique for secure transmission and privacy

Amit K. Shakya1 | Ayushman Ramola1 | Anurag Vidyarthi2

1Electronics and Communication Engineering, Sant Longowal Institute of Engineering and Technology, Longowal, Punjab, India
2Electronics and Communication Engineering, Graphic Era (Deemed to be University), Dehradun, Uttarakhand, India

Correspondence
Ayushman Ramola, Microwave and Broadband Photonics Communication Lab, Department of Electronics and Communication Engineering, Sant Longowal Institute of Engineering and Technology, Sangrur, Punjab, India. Email: xlayushman@gmail.com

Abstract
In this research work, we have developed a new image encryption-based algorithm for Landsat 8 satellite images. Image statistical parameters related to first-order image statistics, that is, mean (μ), SD (σ), and variance (σ²) are used to obtain the feature values for both original images and their encrypted versions. Multispectral satellite images generally contain a wide range of bands, which is 9 to 11 specifically for the Landsat 8 satellite. Hence, the information content of these images is richer than typical images. Through this algorithm, we aim to reduce the image content by randomly selecting only 10% of the total image pixels. These pixels are used to create new images, the so-called encrypted images. The visual presentation of the encrypted image resembles a noisy picture. First-order image statistics are calculated for both original images and their encrypted counterparts. These parameters show a similarity in their numerical values for both original and encrypted images. Thus, noisy pictures can be used for transmission in place of the original image when an outcome is decided through statistical image features. The visual similarity in the original images and encrypted images is obtained from the histogram signature plot for both original and encrypted images. The proposed algorithm can hence be used to convert image data for secure transmission and privacy.

KEYWORDS
image encryption, Landsat 8, mean, multispectral, SD, variance

1 INTRODUCTION

An image is equivalent to millions of words. Digital images are considered as a natural source for information and data exchange from one place to another. Therefore, the use of digital images has proved as an efficient and convenient approach for information interchange. Today in this internet era, enormous data is generated, stored, and circulated every day in the form of digital images. Due to excessive use of high-resolution cameras, image scanners, surveillance drones, remote sensing satellites, and so on the content of digital image data is increasing rapidly. Various domains such as art
collections, architectural designs, engineering designs, remote sensing applications, intellectual property, medical diagnosis, and so on have developed large image databases. Searching an image of interest in an extensive database without any appropriate strategy or judgment is just like searching a needle in a haystack.

Due to the requirement of proper image matching and retrieval tool, “content-based image retrieval (CBIR)” system has been developed. Earlier some traditional methods of searching images in databases depend on the number of descriptive keywords associated with each image. This approach was known as the “text-based approach”. There are two main shortcomings of this approach, that is, first, it requires a considerable level of human labor, time and cost for searching images, and second, examines results are sometimes inaccurate because the text-based approach is subjective. With the passing time and increase in the size of the databases, the text-based approach becomes out-dated. The disadvantages of the text-based retrieval system are overcome by the CBIR system, which was introduced in 1980.

CBIR is an image retrieval system designed to search, browse, and retrieve images from large databases of digital images. CBIR system is a competent scheme used as an alternative for “text-based image retrieval” systems. In the CBIR approach, visual features are extracted from the query image. Retrieval of images is performed by comparing and matching the optical characteristics of the query image with the images stored in the databases.

Figure 1 presents an overview of the searching algorithm process. In which first, a user makes a query of a particular object (image) in the image database. In this database, there are several types of images. Then the role of the search algorithm comes in the picture. The query image is searched within the database by comparing the visual features of the original image with the optical characteristics of the images present in the database. Finally, a picture of interest is obtained, which is displayed to the user for further action. Researchers are working on getting close to perfect image matching by introducing new parameters and putting as minimum input. The proposed “modified private content-based image retrieval (M-PCBIR)” algorithm is an example of this.

The steps involved in the process of the CBIR system are listed as follows.

(a) The user provides a specimen of the original image or query image.
(b) The specimen of the query image is submitted to the search engine.
(c) Once the user submits the query image, the system will search the image in the database according to different searching algorithms applied to achieve satisfactory retrieval performance.
(d) The relevant images identical to the query image are rebound to the user.

The capacity of the data storage in large databases has become a crucial problem, and when it comes to satellite images, this problem becomes more intense. Since we are aware of the fact that satellite images require a large amount of storage space, initially, there were single-band images, but now comes a multispectral image, which contains a combination of \(8 - 11\) different bands. Various bands contain information for different purposes. Thus, all the bands are fused to obtain a multispectral image. The main advantage of these multispectral images is that they provide information about various events through a single platform. Thus, the storage space requires by multispectral images is large as compared with single-band images. These images also need a large amount of data to get a transfer from one place to another place. CBIR systems have a drawback of privacy-related issues since all the queries are openly

**FIGURE 1** General diagram of search algorithm process
searched through search engines over the internet. This shortcoming gives birth to private content-based image retrieval (PCBIR) systems. Many organizations in the corporate world have developed their PCBIR systems such as Viraz Incorporation, International Business Machine, Media Site Incorporation, Facebook, Google, and so on. The main objective of PCBIR systems is to protect confidential data from cyber mugging and digital hacking by making queries through statistical features.

So in this research work, we have added a new feature in the existing PCBIR system, that is, “minimum pixel selection (MPS).” The MPS method requires only randomly selected pixels from the original image to create an encrypted image that is used as a query over the internet. The proposed algorithm has features such as a simple structure, less data usage, overcoming various security threats, and encryption power. We know that satellite images require ample storage space, so we have used multispectral data acquired from currently active “Landsat 8 operational land imager (OLI)” sensor. It is having a combination of 11 different bands. The data obtained by this satellite acquires a large amount of storage space. Here, we will like to inform readers that we are using multispectral Landsat images due to its unique features such as resolutions, pixel counts, dimensions, and so on. These images are encrypted just to show the encryption power of the proposed algorithm. This type of encryption methodology can be used for covert military operations. Else encrypting satellite images is not required.

Here, we have developed a novel algorithm based on the “statistical parameters related to first-order image statistics,” that is, mean (μ), SD (σ), and variance (σ²) and named it as the “M-PCBIR” system. Through this algorithm, we have covered three different objectives.

- We are reducing the pixel count of the original image.
- We are maintaining the privacy of the data by performing random permutation of image pixels.
- We are finally equating the original and encrypted images with each other through first-order statistical feature values.

In the suggested algorithm, first, the classification of the multispectral image dataset is performed based on first-order image statistics. Second, these images are encrypted by selecting only 10% of the random pixels from the total image pixels. These pixels are stored in a new image matrix. This random arrangement of image pixels does not reveal their original identity, and it appears like a noisy image. First-order statistical parameters are calculated for both the original and encrypted images. Both images show a similarity in the feature values. The visual similarity in the original images and their encrypted versions is obtained through histogram signature plots. Similarity plotting is performed to visualize the closeness in the feature value of “mean” and “SD” for both original images and encrypted images, respectively.

The objective of this research work is to hide the information and data during transmission from an unknown hacker. For secure transmission identity of the original data is not revealed and for transmission purpose only encrypted version of the original data is used which look like noise. Both the sender and the receiver end have complete information about the data, their statistical features, and parameter values. Therefore, when encrypted data reach the receiver end through parameter comparison and histogram visualization, the original identity of the data is revealed. Finally, images of interest are extracted from the complete dataset.

The article is organized in eight different sections. Section 2 provides an overview of the NASA Landsat program. Section 3 explains the proposed algorithm of data reduction. Section 4 provides details about the mathematical model of the proposed algorithm. Section 5 presents experimental results using Landsat 8 images. Section 6 presents the implementation results of the proposed algorithm on different types of images. Section 7 offers a discussion of the research work and future scope. Finally, in Section 8, concluding remarks on the research work are presented.

2 | OVERVIEW OF NASA LANDSAT PROGRAM

The query images or input images used in this research work are obtained from “NASA (National Aeronautics and Space Administration) Earth Observatory”. These images are multispectral, having large dimensions, and pixel count. So in this section, we are presenting a summary of the NASA Landsat program and the color composite combination of its spectral bands. Landsat satellite program is considered one of the most successful commercial satellite programs in the history of NASA.
bomb under the vision of “Stewart Udall”. He quoted that “I thought an Earth applications program was a perfect means of bringing the benefits of space back to Earth”. The Apollo mission was the inspiration behind the advancement of the Landsat program. At the time of the Apollo mission, the images of the Earth’s surface were taken for the very first time. Initially, the objective of the launch of the Landsat program was to investigate the availability of Earth resources at different places. This objective gives birth to Landsat 1, which was equipped with a camera mounted on satellite for Earth imaging. It was launched on July 23, 1972 and got decommissioned on January 6, 1978. Figure 2 represents the launch year, and decommissioned year of various Landsat satellites launched to date.

As the Landsat program progressed, the camera was replaced by sensors with multiple bands, which increase not only the resolution but also the size and dimension of the images. Till now, NASA has successfully dispatched 8 Landsat
satellites. On October 5, 1993, NASA launched Landsat 6, which was unfortunately not able to reach its orbit and thus become a single failed Landsat mission. On March 1, 1984, NASA launched Landsat 5. It was a lower Earth orbital satellite, whose main objective was to gather information about Earth surfaces through multispectral images. It has snapped record 2.5 million multispectral images. It provided its services for 29 years and got retired on June 5, 2013. It carries the thematic mapper sensor, which was having the ability of multispectral scanning. Landsat 5 also holds a Guinness record of the longest-operating Landsat satellite, which provided its service for 29 years.

Currently, Landsat 8 is operational, which was launched on February 11, 2013. The principle of this satellite is to ensure the continuous acquisition of Earth imagery. Landsat 8 carries the “OLI and thermal infrared sensor,” it contains a fusion of nine spectral bands and two thermal infrared bands. Figure 3 presents detailed information about operating wavelength (μm) and resolution (m) for different Landsat 8 spectrum bands.

Finally, NASA is planning to launch its latest Landsat 9 mission in late 2020 or early 2021. It may be possible that due to COVID 19 situation, the satellite launch gets postpone. It will carry two sensors “thermal infrared sensor 2 and operational land imager 2”. It is designed for the work period of 5 years and will snap 700 scenes per day.

Multispectral images consist of several bands. These bands are stacked together to form color composite images. If we consider only a single band of the image, it will appear like a grayscale image. Light consists of three primary colors popularly known as RGB, that is, Red-Green-Blue. Computer screens can display images having a combination of these three colors band. When we combine these color bands, the result is a colored image having three primary color and their combination. Figure 4 represents the color composite representation using RGB. Different colors can be created by combining these primary colors in an appropriate format.

The color band for the multispectral Landsat 8 images also consists of these three primary colors. Since in Landsat 8 bands can be fused to develop a new image. The band combination of the Landsat 8 for obtaining a new composite is shown in Table 1.

Figure 5 represents the Landsat 8 image of “Crater Lake National Park,” situated in southwestern Oregon, acquired in March 2014. The combination of different bands of the Landsat 8 for this image is shown in Figure 5B-H, where one band is stacked over the other bands to create a new image. Here, we are performing the color composite operation on different

![Figure 4](image)

**TABLE 1** Band combination of Landsat 8 bands for different color composite

| S.no | Composite name                              | Landsat 8 band |
|------|--------------------------------------------|----------------|
| 1    | Natural-color                              | Fourth Third Second |
| 2    | False-color                                | Seventh Sixth Fourth |
| 3    | Color infrared                             | Fifth Fourth Third |
| 4    | Color composite for agriculture            | Sixth Fifth Second |
| 5    | Color composite for healthy vegetation     | Fifth Sixth Second |
| 6    | Color composite for land and water         | Fifth Sixth Fourth |
| 7    | Color composite for vegetation             | Sixth Fifth Fourth |
| 8    | Short wave infrared                        | Seventh Fifth Fourth |
bands of Landsat 8. The output images are having a combination of various bands and give different visualization every time.

From the available literature, different scientists have reported that the color of a multispectral image is dependent on the amount of “contrast” in that image. Therefore, while converting a multispectral image to another form, the contrast value is going to get most affected.

3 | PROPOSED ALGORITHM OF DATA REDUCTION AND PRIVACY

The proposed “M-PCBIR” algorithm work on the principle of data conversion and hiding. It is the advanced version of PCBIR and thus named as M-PCBIR. The step-wise working of the proposed algorithm is discussed in detail in steps (1-9) followed by its flowchart representation shown in Figure 6.

**Step 1: Selection of the input query image**

The first step is to select the query image. The query image can be of any dimension and resolution. Scale and size limitation of the query image is not a considering factor in the proposed framework. Multispectral Landsat 8 images are used as query images in this experiment.

**Step 2: Conversion of the image to grayscale**

The second step involves the conversion of a multispectral color scale image to grayscale. Multispectral space consists of hue, saturation, and value (HSV). Hue is the measure of the actual wavelength of the color. Saturation describes the quantity of white light present in the shade. Value is the representation of the color intensity. Converting images from multispectral to grayscale eradicate the hue and saturation information while retaining the intensity value information.

**Step 3: Alter the pixel position of the query image**

Any image is composed of a finite number of pixels, each of which has a particular location and purpose for producing meaningful information. In the third step, the random permutation is applied to the image pixels to scramble the position of the pixels and exploit their spatial relationship. Experimental results have proved that such a random arrangement of pixels shows excellent resistance against Brute force and many other security attacks. The properties of the proposed cryptography are as follows.

(a) Random permutation encryption is deterministic, which is determined by the mathematical equations ruling their behavior.

(b) They are visually unpredictable and lead to significant changes in the visual characteristics of images.

(c) The image appears as noise, but the noisy encrypted image has a specific sense of statistical properties.
**Step 4: Select only 10% of pixels from the original image**

In the fourth step, we have selected only 10% of the total image pixels, which are stored in a matrix form. Let an original query image is having a dimension of $2000 \times 3000$, thus have a total of $6\,000\,000$ pixels, 10% of total pixels, that is, $600\,000$ pixels are selected and stored in the matrix form. A new image composed of 10% of the total pixels will strengthen the encryption level and saves not only the storage space but also reduce transmission time. This image is named as an encrypted image in this research work.

**Step 5: Store pixel in a separate matrix**

The most common characteristic features of the image are color, texture, and shape. They are also known as low-level visual features. We are extracting texture features information from the image by statistical methods. The first-order gray level statistics are formed by the information provided by intensity histogram. The main reason behind choosing histograms for extracting texture features is that first-order statistics are independent of the neighboring relationship between pixels of the image.

**Step 6: Calculate first-order statistical features for the original image (Step 1)**

The first-order image statistics such as mean ($\mu$) and SD ($\sigma$) are computed for the original (query) image. All the pixels in the original image are at a specific position to visually represent meaningful information. The first-order image statistics are obtained for all the Landsat 8 images used in this research work.

**Step 7: Calculate first-order image statistical features for the encrypted image (Step 4)**

An encrypted image is formed by only 10% of the total image pixels. Statistical features mean ($\mu$) and SD ($\sigma$) are computed for the encrypted image. These statistical features show approximately the same numerical values as the original images. Statistical properties remain unaffected by the changes that take place by changing the arrangement order of image pixels. 10% of the total image pixels are stored in the matrix form. The values of the statistical features obtained from these images are later used to make an identification with the original image.
**Step 8: Perform feature matching in between the original images and encrypted images**

Finally, the statistical features of the original images and the encrypted images are compared with each other, which shows similarity in the feature value. The amount of difference generated between both values is quite small and even less than (1%). Thus, through statistical feature values identification between the original and the encrypted images can be performed.

**Step 9: Identify original images from the encrypted image**

Finally, through the numerical value of the statistical features “mean” and “SD,” we can identify the original image and its encrypted version.

The flowchart of the planned M-PCBIR algorithm is shown in Figure 6.

Multispectral images are converted to a grayscale image by the “Di Zenzo structure tensor matrix.” These images contain information about HSV for any scene. When multispectral images are converted to a grayscale image, the following important points are to be kept in consideration.

- The luminance of the RGB color triplets is mapped in color independent spatial direction.
- The information about the saturation and hue is discarded, and the only luminance information is kept into consideration.

There are several methods described to separate luminance information from hue and saturation, for example, YIQ, HSV, LHS, CIELab,35,36 and so on. The grayscale images store luminance information effectively within themselves, whereas the multispectral images are converted to grayscale by preserving the image “contrast.” Here, we are explaining the conversion procedure of multispectral image to grayscale using the “Di Zenzo Structure tensor matrix”.37,38

Consider an image \( I \) in a rectangular grid format and expressed as \( \Omega = \{1 \ldots m\} \times \{1 \ldots q\} \). Let \( P: \Omega \cong M^m \) be a multispectral image.

\[ G: \Omega \cong \{1 \ldots m\} \times \{1 \ldots q\} \cong M \] be a grayscale image.

For a multispectral image, two components of the gradient for channel \( l = \{1 \ldots n\} \) are given by Equations (1) and (2), respectively.

\[ \rho^l_x = \delta_x P(x, y, l), \]  
\[ \rho^l_y = \delta_y P(x, y, l), \]  

which represents the partial derivatives of the components.

Likewise, the grayscale derivative of the image \( I \) in the vertical and horizontal direction is represented by Equations (3) and (4), respectively.

\[ g_x = \delta_x g(x, y), \]  
\[ g_y = \delta_y g(x, y). \]  

For a multispectral image, Di Zenzo’s tensor structure of \( 2 \times 2 \) for each pixel can be created and expressed by Equation (5).

\[ Z(x, y) = \begin{pmatrix} \sum_{l=1}^{n} \rho^l_x \rho^l_y & \sum_{l=1}^{n} \rho^l_x \rho^l_y \\ \sum_{l=1}^{n} \rho^l_x \rho^l_y & \sum_{l=1}^{n} \rho^l_y \rho^l_y \end{pmatrix}. \]  

Since \( Z \) is a symmetric matrix having an orthogonal matrix \( V \) with column \( v \), it is represented by Equation (6).

\[ Z(x, y) = v_i \lambda_i v_i^T, \]  

Here, we have observed that the eigenvector corresponding to the most significant eigenvalue point in the direction of the maximum “contrast.”
The “De Zenzo Matrix” representation for the grayscale image is expressed by Equation (7).

\[
Z_g(x, y) = n \begin{pmatrix}
g_x g_x & g_x g_y 
g_x g_y & g_y g_y
\end{pmatrix}.
\]

(7)

With \( n \) to match \( Z \) from Equation (5) for the multispectral image. The eigenvalue decomposition is applied which is \( Z_g \) expressed by the Equation (8).

\[
Z_g(x, y) = u_i \gamma_i u_i^T, \quad i = 1, 2.
\]

(8)

To overcome the issue of matching contrast between \( Z \) and \( Z_g \). Socolinsky and Wolff\(^{39}\) concluded that the optimal gradient for generating an output grayscale images is in the direction of the maximum eigenvalue direction, that is, \( v = v_1 \). Thus, they defined contrast of the individual pixel as expressed by Equation (9).

\[
C_m(x, y) = \pm \sqrt{\lambda_1} v_1.
\]

(9)

Energy function (\( W \)) is expressed by Equation (10).

\[
W = \sum_{i=1}^{m} |C_g - C_m|^2.
\]

(10)

The best quadratic grayscale approximation \( g \) of \( P \) is that which minimizes the value of \( W \). Thus, a solution is obtained as \( C_g = C_m \). We are aware that the sign in the Equation (9) is not defined, but it should be dependent on the “contrast” of the image. Finally, two conclusions are obtained to determine image contrast.

- Image contrast is dependent on the eigenvector associated with the maximum eigenvalue.
- The sign of the contrast can be obtained by considering the contrast in the luminance channel.

### 4 MATHEMATICAL MODELLING OF THE PROPOSED ALGORITHM

The standard probability distribution model\(^{40-42}\) for estimating the probability of occurrence of an individual pixel within an image is given by Equation (11).

\[
f \left( \frac{x - \mu}{\sigma} \right) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(x-\mu)^2}{2\sigma^2}},
\]

(11)

where \( \mu \) represents the mean or expectation of the normal distribution.

\( \sigma^2 \) represent the variance of the probability distribution.

\( \sigma \) is the SD of the probability distribution.

\( x \) is the central value of the probability distribution.

Let a query image contains a total of \( m \times n \) pixels. These pixels are arranged in the form of the matrix at a specific position to represent meaningful information. This information can be in the form of an image, data, and so on. The matrix representation of the pixels, when arranged in a planned manner to constitutes meaningful information, is shown in Equation (12).

\[
I(\text{original}) = \begin{bmatrix}
p(1, 1) & p(1, 2) & p(1, 3) & \cdots & p(1, n-2) & p(1, n-1) & p(1, n) 
p(2, 1) & p(2, 2) & p(2, 3) & \cdots & p(2, n-2) & p(2, n-1) & p(2, n) 
p(3, 1) & p(3, 2) & p(3, 3) & \cdots & p(3, n-2) & p(3, n-1) & p(3, n) 
p(4, 2) & \ddots & & \cdots & p(4, n-2) & p(4, n-1) & p(4, n) 
\vdots & \ddots & \ddots & \ddots & \vdots & \vdots & \vdots 
p(m-2, 1) & p(m-2, 2) & p(m-2, 3) & \cdots & p(m-2, n-2) & p(m-2, n-1) & p(m-2, n) 
p(m-1, 1) & p(m-1, 2) & p(m-1, 3) & \cdots & p(m-1, n-2) & p(m-1, n-1) & p(m-1, n) 
p(m, 1) & p(m, 2) & p(m, 3) & \cdots & p(m, n-2) & p(m, n-1) & p(m, n)
\end{bmatrix}.
\]

(12)
These pixels can be arranged in a single row vector through which the random selection of the image pixel is performed. Assuming MPS, we have considered only 10% randomly selected image pixels from the total image pixels. An example of an image matrix representing the random pixel distribution is shown in the Equation (13).

Here 10% of pixels are arranged in a completely random manner so that no information can be obtained from them. Every single time when the pixels are arranged randomly to form an image matrix, the visualization of the image matrix will be different from the previous one. Similarly, the visual representation of the encrypted images will also be diverse every time.

$$I(\text{encrypt}) = \begin{bmatrix}
p(m, n - 8) & p(m, n - 2) & \cdots & p(m - 2, n - 1) & p(4, n - 1) \\
p(m - 12, n - 13) & p(m - 1, n - 2) & \cdots & p(m - 1, n - 3) & p(m - 1, n - 1) \\
\vdots & \ddots & \vdots & \ddots & \vdots \\
p(m - 4, n - 4) & p(m - 3, n - 44) & \cdots & p(m - 1, n - 7) & p(m - 1, n - 1) \\
p(m - 2, n - 23) & p(m - 7, n - 63) & \cdots & p(m - 2, n - 2) & p(m - 13, n - 12)
\end{bmatrix}.$$  

First-order image statistics include mean, variance, and SD are obtained for both original and encrypted images. Let an original query image contains a total of "q" pixels then these first-order image statistics features, that is, mean ($\mu_{\text{original}}$), variance ($\sigma_{\text{original}}^2$), and SD ($\sigma_{\text{original}}$) is expressed by Equations (14) to (16), respectively. Where $p(z)$ represents a pixel position.

$$\mu_{\text{original}} = \sum_{z=0}^{q-1} r_z \times p(z), \quad (14)$$

$$\sigma_{\text{original}}^2 = \sum_{z=0}^{q-1} (r_z - \mu)^2 \times p(z), \quad (15)$$

$$\sigma_{\text{original}} = \sqrt{\sigma^2}, \quad (16)$$

The encrypted image contains only 10% of the total image pixels, that is, “10% of the q” pixels. The mean ($\mu_{\text{encrypt}}$), variance ($\sigma_{\text{encrypt}}^2$), and SD ($\sigma_{\text{encrypt}}$) for the encrypted image are expressed by Equations (17) to (19), respectively.

$$\mu_{\text{encrypt}} = \sum_{z=0}^{10\% \text{of} (q-1)} r_z \times p(z), \quad (17)$$

$$\sigma_{\text{encrypt}}^2 = \sum_{z=0}^{10\% \text{of} (q-1)} (r_z - \mu)^2 \times p(z), \quad (18)$$

$$\sigma_{\text{encrypt}} = \sqrt{\sigma^2}, \quad (19)$$

The optimum number of the image pixels used for the encryption purpose is extracted from the total image pixels using random permutation of the image pixels. A total of only 10% of the image pixels are extracted from the image to create an encrypted image. In the image encryption process, a random permutation of the image pixel is performed to obtain a completely secure encrypted image.

In image processing applications, three types of permutations can be applied, that is, pixel permutation, bit permutation, and block permutation. A digital image is formed by pixels, which itself is the combination of the 8 bits. Random permutation in bits is performed using an encryption key. The size of the encryption key performing bit permutation is 8 bit. Thus, the total number of the available keys is 8!, that is, 40 320. The process of performing permutation in the image pixels is known as pixel permutation. Pixel permutation is applied to the image using the key size in two possible ways.

- If the key size is 1D (one dimensional), then the column and row permutation can be performed.
- If the key size is 2D (two dimensional), then pixels are placed at some specific positions.

It is also possible to divide an image into a subblock. Block permutation is used permute subblocks. This permutation is applied to an image using the following steps.
A multispectral image of size \((m, m)\) is taken and then decomposed in \(X\) and \(Y\) number of subblocks for rows and columns, respectively. Each subblock is having a size of \((n, n)\), and each pixel of the subblock has been assigned a position varying from \((1, 1)\) to \((n, n)\).

Now, the 2D encryption key of size \((n, n)\) is used to apply permutation on image pixels to each subblock, which itself is the combination of the random numbers at distinct positions.

The encryption key is used to map the position of row and column for the pixel of the subblock. Pixel positions can be determined from Equations (20) and (21), respectively.

\[
\begin{align*}
    r &= \text{floor}\left(\frac{k_{(n,n)}}{n}\right) + 1, \\
    c &= \text{mod}\left((k_{(n,n)}, n)\right) \text{ provided } c \neq 0
\end{align*}
\]

where \(r\) and \(c\) represent the position of the row and column, respectively, where the pixel is to be placed. \(k_{(n,n)}\) represents the random number of pixel positions corresponding to the encryption key.

After the completion of the pixel permutation, subblock is combined and assigned position number from row to column starting from \((1, 1)\) to \((x, x)\) which is only 10% of the total image pixels.

Thus, we get an encrypted image by performing pixel and subblock permutation using an encryption key.

5 Experimental Results

The images used in this research work are multispectral. They are obtained from the currently active Landsat 8 OLI sensor. Still, the proposed algorithm has the potential to be applied to all types of images, which is the strength of the algorithm. The reason for using satellite imagery is that they have a number of properties such as five different types of resolution, that is, spatial, spectral, temporal, radiometric and geometric, large dimensions, multispectral nature, and so on. In this experiment, we have taken 24 multispectral Landsat 8 images acquired from its OLI sensor. It contains a fusion of 11 different bands, that is, “Coastal/Aerosol, Blue, Green, Red, Shortwave Infrared (SWIR 1), Shortwave Infrared (SWIR 2), Panchromatic, Cirrus, Thermal Infrared (TIRS 1), and Thermal Infrared (TIRS 2)”. The details regarding these bands, their operational wavelength, and resolution can be obtained from Figure 3. Since all the pixels present in the image are at specific positions, thus the images present meaningful information. This critical information is the visual appearance that is represented in the form of multispectral Landsat images shown in Figure 7.

Now the pixels present in these images are arranged randomly to represent image with no meaningful information. These types of images are called encrypted images in this research work and are shown in Figure 8. The randomly arranged image pixels do not reveal the original content of the image. Thus, only the user performing this operation is aware of the original content of the data and its converted version. This methodology maintains the privacy of the image data completely as the identity of the original data remains unknown for everyone else other than the programmer itself.

5.1 Encrypted version of the original images along with the pixel count

The first-order image statistical parameters are calculated for the original image and their encrypted versions. Encrypted images are formed by randomly selecting 10% of the total image pixels. Images created by 10% of the total pixels do not reveal any information. These images have obtained approximately the same statistical values as the original images. The obtained numerical values of the statistical features for both versions (original and encrypted) are shown in Table 2.

The dissimilarity in the numerical values of the statistical features mean, and the SD is less than (1%). Thus, based on statistical features values, original and encrypted images can be considered synonyms of each
FIGURE 7  A, Barefoot Bay, B, California, C, Charlotte Bay, D, Collbran, E, Colorado River, F, Copper River, G, Cotahuasi, H, Dasbrancas, I, Dmv, J, Entoole, K, Fuego, L, Hps, M, Ivanpah, N, Katahdin, O, Kazakhastan, P, Sakurajima, Q, Sfbay, R, South Korea, S, Tanezrouft, T, Thames, U, Topaz, V, Valley Fire, W, Wrangel Glacier, X, Pine Island Glacier47
FIGURE 8  Encrypted version, A, Barefoot Bay, B, California, C, Charlotte Bay, D, Collbran, E, Colorado River, F, Copper River, G, Cotahuasi, H, Dashbrancas, I, Dmv, J, Entoole, K, Fuego, L, Hps, M, Ivanpah, N, Katahdin, O, Kazakhstan, P, Sakurajima, Q, Sfbay, R, South Korea, S, Tanezrouf, T, Thames, U, Topaz, V, Valley Fire, W, Wrangel Glacier, X, Pine Island Glacier.
FIGURE 8 continued
Encrypted Image (Q), Total Pixels (1073217)

Encrypted Image (R), Total Pixels (1257472)

Encrypted Image (S), Total Pixels (1600000)

Encrypted Image (T), Total Pixels (4900000)

Encrypted Image (U), Total Pixels (1600000)

Encrypted Image (V), Total Pixels (1225000)

Encrypted Image (W), Total Pixels (51840)

Encrypted Image (X), Total Pixels (4012823)

FIGURE 8 continued
other. The visual similarity in the original image and their encrypted version is obtained from the histogram signature plots.

### 5.2 Histogram signature plot for the original image and their encrypted version

Here, we have plotted the histogram signature plot for the original and encrypted images. The histogram is a computer-generated approximate representation of numerical data. The histogram of the original image and its encrypted version show similarity with each other. The images formed by using only 10% of pixels show a similar histogram as compared with its original image. Thus, through histogram plots, we have obtained visual similarity in the original image and their encrypted version. Histogram signature plots for the original image and its encrypted version are shown in Figure 9.
FIGURE 9  Histogram signature plot of original image and their encrypted version, A, Barefoot Bay, B, California, C, Charlotte Bay, D, Collbran, E, Colorado River, F, Copper River, G, Cotahuasi, H, Dasbrancas, I, Dmv, J, Entoole, K, Fuego, L, Hps, M, Ivanpah, N, Katahdin, O, Kazakhastan, P, Sakurajima, Q, Sfbay, R, South Korea, S, Tanezrouft, T, Thames, U, Topaz, V, Valley Fire, W, Glacier, X, Pine Island Glacier
FIGURE 9 continued
FIGURE 9 continued
Now the similarity plot in between mean and SD for the original image and encrypted image are plotted together. This confirms that the parameters mean and SD have obtained approximately the same numerical values. The similarity plotting for both of the statistical parameters are shown in Figure 10A,B, respectively. Thus, both the images can be used in place or each other when it comes to reaching an outcome through statistical features values. Thus, from the proposed encryption algorithm, we can encrypt our data for secure transmission. Reducing the content of data enhances the transmission rate; therefore, the proposed algorithm can be used further for reducing the content of various types of images such as RGB images, DICOM images, hyperspectral images, and so on.

6 IMPLEMENTATION OF THE PROPOSED ALGORITHM ON OTHER TYPES OF IMAGES

In this section, we have tested the potential of the proposed algorithm for encrypting different types of images. These images are of different formats, sizes, and dimensions. The encryption of these images does not provide any information about the original identity of the image. First-order image statistics are obtained for both the original query image and their encrypted versions. The sample images used in this section are shown in Figure 11. These sample’s images include Penguins, Tulips, Coronavirus, X-Ray, Lena, Mandril, Koala, and UV COVID 19.
Now the image pixels are randomly arranged to represent an image with no useful information. These images are called encrypted images and are shown in Figure 12. These images do not reveal any information thus can be used for secure transmission and privacy in the place of the original image.

The first-order image statistics, that is, the mean and SD for the original image and their encrypted versions formed by only 10% of the total image pixels, are represented in Table 3. Here it is observed that the algorithm is working efficiently on all other types of images other than multispectral satellite images.

The visual similarity between both versions of images is represented by the histogram signature plot shown in Figure 13.

Now the efficiency of the proposed algorithm is examined for the images of minimal dimensions. Since the dimension of the satellite images are very large, and 10% of random pixels are also huge. Thus, to observe the behavior of the proposed algorithm for the small images, we have included four different images of small size as a scooter, black Taj Mahal, postcards, and Jesus, as shown in Figure 14.

Now we have randomly arranged 10% pixels from the total image pixels to visually represent an encrypted image, as shown in Figure 15.

The first-order image statistics, mean, and standard deviation for the original small images and their encrypted versions are represented in Table 4.

The visual similarity in the original images and their encrypted versions is represented by histogram signature plots for both original and encrypted small images, as shown in Figure 16.

These plots show similarity in the visual appearance of the images. Still, now we have visually observed slight changes in the histogram of the encrypted images as they began to show sharp peaks when compared with the histogram signature plots of there original images.

From this investigation, we have observed that the proposed method also applies to images of small dimensions. The statistical features “mean” have obtained approximately the same value. The value of the statistical feature “SD” slightly differ for the image postcard.

Finally, a question arises whether there should be any restriction on the size of the query image or what should be the size of the query image. This issue is addressed by taking two images of different dimensions. The first one is a high-resolution multispectral image having a large number of pixels, and the second one is the low-resolution image with relatively less number of pixels. For both the images, encryption is performed by taking 90% – 5% of the total pixels of the original image. Thus, we can get the answer to this query.

The size of the multispectral image of the river Nile showed in Figure 17A is 7540 × 5694, that is, it contains a total of 42 932 760 pixels. The second image of the apple, shown in Figure 17B is having a dimension of 259 × 195. It includes a total of 50 505 pixels. Here, we are looking for optimum encryption by taking the least number of image pixels. Thus, both the images are encrypted by taking 90% – 5% of the total image pixels. Encrypted versions of the River Nile are shown in Figure 18A-J.
FIGURE 12  Encrypted version, A, Penguins, B, Tulips, C, Coronavirus, D, X-Ray, E, Lena, F, Mandril, G, Koala, H, UV COVID 19
### Table 3

Image dimensions, total pixels, and first-order statistical values of the mean (μ) and the SD (σ) for original and encrypted images

| S.no | Objects   | Image dimension | Total pixels | First-order image statistics (Original image) | First-order image statistics (10% of TP) |
|------|-----------|-----------------|--------------|---------------------------------------------|----------------------------------------|
|      |           |                 |              | Mean (μ)  | SD (σ)  | Mean (μ)  | SD (σ)  |
| (a)  | Penguins  | 1024 × 768      | 786,432      | 148.009 | 11.3997 | 147.663  | 11.38   |
| (b)  | Tulips    | 1024 × 768      | 786,432      | 123.76  | 11.2191 | 122.017  | 11.1657 |
| (c)  | Coronavirus| 875 × 875       | 765,625      | 145.656 | 11.1145 | 144.859  | 11.1703 |
| (d)  | X-Ray     | 1024 × 768      | 786,432      | 56.0754 | 9.0897  | 56.4361  | 9.1015  |
| (e)  | Lena      | 1500 × 1000     | 1,500,000    | 93.5687 | 9.46728 | 92.1111  | 9.49403 |
| (f)  | Mandrill  | 1024 × 768      | 786,432      | 71.663  | 9.46342 | 71.6617  | 9.48698 |
| (g)  | Koala     | 1024 × 768      | 786,432      | 114.035 | 10.2709 | 114.401  | 10.3731 |
| (h)  | UV COVID 19| 875 × 875       | 765,625      | 171.195 | 11.0025 | 173.012  | 10.9491 |

**Figure 13** Histogram plotting in between the original image and their encrypted version, A, Penguins, B, Tulips, C, Coronavirus, D, X-Ray, E, Lena, F, Mandrill, G, Koala, H, UV COVID 19
### Table 4

Image dimensions, total pixels, and first-order statistical values of the mean ($\mu$) and the SD ($\sigma$) for original and encrypted small images.

| S.no | Objects       | Image dimension | Total pixels | First-order image statistics | First-order image statistics (10% of TP) |
|------|---------------|-----------------|--------------|------------------------------|----------------------------------------|
|      |               |                 |              | Original image               | (10% of TP)                            |
|      |               |                 |              | $\mu$ | $\sigma$ | $\mu$ | $\sigma$ |
| (a)  | Scooter       | $200 \times 150$ | 30 000       | 155.519 | 11.0511 | 155.004 | 11.065 |
| (b)  | Black TajMahal| $320 \times 240$ | 76 800       | 122.278 | 9.79718 | 122.212 | 9.77418 |
| (c)  | Postcard      | $225 \times 225$ | 50 625       | 205.982 | 8.80134 | 205.327 | 9.11809 |
| (d)  | Jesus         | $236 \times 316$ | 74 576       | 91.629  | 9.65572 | 89.7187 | 9.62766 |

**Figure 14** Small images, A, scooter, B, black TajMahal, C, postcard, D, Jesus.

**Figure 15** Encrypted version, A, scooter, B, black TajMahal, C, postcard, D, Jesus.
FIGURE 16  Histogram signature plotting in between the original image and their encrypted version, A, scooter, B, black TajMahal, C, postcard, D, Jesus

FIGURE 17  A, Multispectral Landsat 8 satellite image of River Nile, B, Apple

Now the apple image is encrypted by taking 90% – 5% pixels from the total image pixels. The encrypted versions of the Apple images are shown in Figure 19A-J.

Here from Figure 18, we have observed that for the multispectral satellite images, the visual appearance of the encrypted images seems to be the same for 90% pixels to 5% pixels. This has happened because satellite images have a huge pixel count. On the other hand, from Figure 19, the visual appearance of the encrypted images has begun to change from 40% pixels onwards. This change in the appearance is quite visible for Figure 19I,J, where the pixel count is only 10% and 5%, respectively. One of the reasons for this change is apple image is having fewer numbers of image pixels as compared with the multispectral image of River Nile.

Thus, based upon observations, we have obtained an optimum value of the image pixels for both large and small dimension images, and it should be 10% of the total image pixels. Satellite images can be further encrypted by reducing more numbers of pixels, but for small images, 10% of the entire image pixels is a reasonable quantity.
It is also important to note that the query image should have at least a minimum number of pixels so that this operation of image encryption can be applied to them. In this experiment, the minimum size of the query image is $259 \times 195$. Thus, from our analysis, we will like to recommend that users can use the proposed algorithm with a query image of at least 50 000 image pixels so that encryption strength should not get affected, and the content of data is not revealed.

**FIGURE 18** Encrypted versions of river Nile by taking 90% to 5% of the total image pixels
7 | DISCUSSION

The proposed scheme of data reduction and hiding is useful for various applications. This algorithm is based on the observations and analysis developed by analyzing multispectral images, RGB images, and DICOM images. Mostly satellite images are used in this research work, but the area of exploration of this algorithm is not limited to satellite images only. All the categories of images can be encrypted through this algorithm. The proposed algorithm is based on the parameters of first-order image statistics, that is, “mean, variance, and SD.” The encrypted images can be considered as noisy images created by using only 10% random pixels from the original images. This method is similar to “pixel scrambling,” which does not change the image histograms. The original image and encrypted image develop the same type of first-order image statistical features, which help to identify original images from the encrypted images. Histogram analysis is done to obtain the visual similarity in the images, which results in the same type of histogram formation between original and encrypted images. It has been recommended to apply the proposed algorithm to images having at least 50,000 image pixels. Thus, the proposed algorithm can be used on many occasions like if someone wants to create encrypted images that look like noisy pictures, they can follow encryption steps to create a noisy image with varying numbers and position of pixels. Similarly, for some users, the visual similarity is obtained through histogram plotting between the original image and encrypted images. Finally, the comparison can also be made between two images based on their statistical values. Thus, the strength of the proposed algorithm is that it contains many steps which can also be used individually as well as entirely according to the need and situation of any user. In the future, a graphical user interface can also be created for automatic selection of the minimum number of pixels from an image and performing random pixel scrambling.
FIGURE 19  Encrypted images of apple by taking 90% to 5% of the total image pixels
CONCLUSION

The proposed scheme is useful in encrypting all types of images such as satellite images, DICOM images, general RGB images, and so on, and converting a meaningful image to a noisy image. Relevant and confidential image data can be easily encrypted and transmitted as noise from the sender to the receiver. Even the statistical parameter values can be used in place of each other. Original image statistical values can be used for encrypted images and vice versa. While performing this experimental work, we have observed a situation that if two images develop the same type of statistical parameter values, then how to identify the original image and its encrypted version. The answer to this through pixels counts and encrypted image appearance; thus, we can locate the original image and its encrypted version. Therefore, the proposed algorithm has the potential to be widely used for image encryption, data hiding, and privacy-related issues.

ACKNOWLEDGEMENT
The authors are thankful to the three anonymous reviewers and journal editor for their comments, concerns, queries, and constructive suggestions.

PEER REVIEW INFORMATION
Engineering Reports thanks Wannida Sae-Tang and other anonymous reviewers for their contribution to the peer review of this work.
AUTHOR CONTRIBUTIONS

Amit K. Shakya: contributed to the conceptualization; data curation; formal analysis; funding acquisition; investigation; methodology; project administration; resources; software; supervision; validation; visualization; writing-original draft; writing-review and editing. Ayushman Ramola: contributed to the conceptualization; data curation; formal analysis; funding acquisition; investigation; methodology; project administration; resources; software; supervision; validation; visualization; writing-original draft; writing-review and editing. Anurag Vidyarthi: contributed to the conceptualization; data curation; formal analysis; funding acquisition; investigation; methodology; project administration; resources; software; supervision; validation; visualization; writing-original draft; writing-review and editing.

CONFLICT OF INTEREST

The authors declare that they have no conflict of interest.

ORCID

Amit K. Shakya https://orcid.org/0000-0002-7710-4276
Ayushman Ramola https://orcid.org/0000-0002-1903-5401
Anurag Vidyarthi https://orcid.org/0000-0002-9045-1782

REFERENCES

1. Goodrum AA. Image information retrieval: an overview of current research. Inf Sci. 2000;3:63-66.
2. Williamson B. Digital education governance: data visualization, predictive analytics, and ‘real-time’ policy instruments. J Educ Policy. 2016;31(2):123-141.
3. Wang HH, Mohamad D, Ismail N. Image retrieval: techniques, challenge, and trend. Int J Comput Electr Autom Control Inf Eng. 2009;3(12):2908-2910.
4. Guglielmo EJ, Rowe NC. Natural language retrieval of images based on descriptive captions. ACM Trans Inf Syst. 1996;14(3):237-267.
5. Araujo A, Girod B. Large-scale video retrieval using image queries. IEEE Trans Circuits Syst Video Technol. 2018;28(6):1406-1420.
6. Liu Y, Zhang D, Lu G, Mah W-Y. A survey of content-based image retrieval with high-level semantics. Pattern Recognit. 2006;40:262-282.
7. Smeulders AW, Worring M, Santini S. Content-based image retrieval at the end of the early years. IEEE Trans Pattern Anal Mach Intell. 2000;22(12):1349-1380.
8. Ishii T, Simo-Serra E, Iizuka S, Mochizuki Y, Sugimoto A, Ishika H. Detection by classification of buildings in multispectral satellite imagery. Paper presented at: 23rd International Conference on Pattern Recognition (ICPR); 2016; Cancun, Mexico.
9. Liu Y, Sun Y, Xie A, et al. Potential of Hyperspectral imaging for rapid prediction of anthocyanin content of purple-fleshed sweet potato slices during drying process. Food Anal Methods. 2017;10(1):3836-3846.
10. Xia Z, Zhu Y, Sun X, Qin Z, Ren K. Towards privacy-preserving content-based image retrieval in cloud computing. IEEE Trans Cloud Comput. 2018;6(1):276-286.
11. Mirhosseini M, Nezamabadi-pour H. BICA: a binary imperialist competitive algorithm and its application in CBIR systems. Int J Mach Learn Cybern. 2018;9(1):2043-2057.
12. Xu Y, Gong J, Xiong L, Xu Z, Wang J, Shi Y-Q. A privacy-preserving content-based image retrieval method in the cloud environment. J Vis Commun Image Represent. 2017;43(1):164-172.
13. Shakya AK, Ramola A, Kandwal A, Chamoli V. Privacy-preserving random permutation of image pixels enciphered model from cyber attacks for covert operations. Commun Comput Inf Sci. 2018;905(1):401-410.
14. Nakamura K, Nitta N, Babaguchi N. Encryption-free framework of privacy-preserving image recognition for photo-based information services. IEEE Trans Inf Forensics Secur. 2019;14(5):1264-1279.
15. Weng L, Amsaleg L, Morton A, Marchand-Maillet S. A privacy-preserving framework for large-scale content-based information retrieval. IEEE Trans Inf Forensics Secur. 2015;10(1):152-167.
16. Saritha RR, Paul V, Kumar PG. Content based image retrieval using deep learning process. Clust Comput. 2019;22(1):4187-4200.
17. Lavorgna A. Cyber-organised crime. A case of moral panic? Trends Organized Crime. 2019;22(1):357-374.
18. Xie H, Luo X, Xu X, Pan H, Tong X. Automated subpixel surface water mapping from heterogeneous urban environments using Landsat 8 OLI imagery. Remote Sens. 2016;8(7):1-16.
19. Rabatel A, Sirguey P, Drolon V, Maisongrande P, Arnaud Y. Annual and seasonal glacier-wide surface mass balance quantified from changes in glacier surface state: a review on existing methods using optical satellite imagery. Remote Sens. 2016;8(7):45-47.
20. Iyer R, Ozer E. Visual IoT: architectural challenges and opportunities; toward a self-learning and energy-neutral IoT. IEEE Micro. 2016;36(6):45-47.
21. Hassanalierragh M, Page A, Soyata T, Sharma G, Aktas M, Mateos G. Health monitoring and management using internet-of-things (IoT) sensing with cloud-based processing: opportunities and challenges. Paper presented at: IEEE International Conference on Services Computing; 2015; New York, NY.
22. Gupta GK, Jha SK. Parallel algorithms for mean, variance, and standard deviation over a 2D-mesh network. Recent Trends Parallel Comput. 2019;6(3):17-22.
23. Yang Y, Barnes C. Approximate program smoothing using mean-variance statistics, with application to procedural Shader Bandlimiting. *Comput Graph Forum*. 2018;37(2):443-454.

24. Przyborski P, Levy R. NASA Earth Observatory, EOS Project Science Office, 1999. https://earthobservatory.nasa.gov/ Accessed March 17, 2020.

25. Wulder MA, Loveland TR, Roy DP, Crawford CJ, Masek JG, et al. Current status of Landsat program, science, and applications. *Remote Sens Environ*. 2019;225(1):127-147.

26. Wood CA. Scientific knowledge of the moon, 1609 to 1969. *Geosciences*. 2019;9(5):1-13.

27. Masek JG, Taylor MP, Rocchio L. Landsat Science, NASA, March 12, 2020. https://landsat.gsfc.nasa.gov/how_landsat_helps/case-studies-2/ Accessed March 16, 2020.

28. Zhu Z, Wulder MA, Roy DP, Woodcock CE. Benefits of the free and open Landsat data policy. *Remote Sens Environ*. 2019;224(1):382-385.

29. Masek JG, Taylor MP, Rocchio L. “Landsat 6,” Earth Resources Observation and Science Center, March 12, 2020. https://landsat.gsfc.nasa.gov/landsat-6/. Accessed March 16, 2020.

30. Egorov AV, Roy DP, Zhang HK, Li Z. Landsat 4, 5 and 7 (1982 to 2017) analysis ready data (ARD) observation coverage over the conterminous United States and implications for terrestrial monitoring. *Remote Sens*. 2019;11(447):1-19.

31. Jing X, Leigh L, Pinto CT, Helder D. Evaluation of RadCalNet output data using Landsat 7, Landsat 8, sentinel 2A, and sentinel 2B sensors. *Remote Sens*. 2019;11(541):1-26.

32. Boryana E, Allen L, Joel MC, Aaron P, Dennis R, Amy S. Landsat 9 TIRS-2 Spectral Response Test: Updates & Perspective. Japan: Goddard Space Flight Center, Yokohama; 2019.

33. Zhu Z, Wulder MA, Roy DP, Crawford P. Automated extraction of visible floodwater in dense urban areas from RGB aerial photos. *Remote Sens*. 2020;12(14):2198.

34. Martínez MÁ, Etchebehere S, Valero EM, Nieves JL. Improving unsupervised saliency detection by migrating from RGB to multispectral images. *Color*. 2019;44(6):1-11.

35. Poddar S, Pedersen M, Karar V. Color image modification with and without hue preservation. *Sensing Imaging*. 2018;19:35.

36. Hameed K, Chai D, Rassau A. A comprehensive review of fruit and vegetable classification techniques. *Image Vis Comput*. 2018;80:24-44.

37. Jung H, Kim Y, Jang H, Ha N, Sohn K. Unsupervised deep image fusion with structure tensor representations. *IEEE Trans Image Process*. 2020;29:3845-3858. https://doi.org/10.1109/TIP.2020.2966075.

38. Yang X, Guo B, Xiao Z, Liang W. Improved structure tensor for fine-grained texture inpainting. *Signal Process Image Commun*. 2019;73:84-95. https://doi.org/10.1016/j.image.2018.02.006.

39. Socolinsky D, Wolff L. Multispectral image visualization through first-order fusion. *IEEE Trans Image Process*. 2002;11(8):923-931.

40. Pollak M, Shauly-Aharonov M. A double recursion for calculating moments of the truncated Normal distribution and its connection to change detection. *Methodol Comput Appl Probab*. 2019;21(1):889-906.

41. Olmos NM, Venegas O. Modified generalized half-normal distribution with application to lifetimes. *Appl Math Inf Sci*. 2018;12(3):637-643.

42. Horrace WC. Moments of the truncated normal distribution. *J Prod Anal*. 2015;43(1):133-138.

43. Iona A, Theodorou A, Watelet S, Troupin C, Beckers J-M. Mediterranean Sea hydrographic atlas: towards optimal data analysis by including time-dependent statistical parameters. *Earth Syst Sci Data*. 2018;10(1):1281-1300.

44. You FM, Song Q, Jia G, et al. Estimation of genetic parameters and their sampling variances for quantitative traits in type 2 modified augmented design. *Crop J*. 2016;4(2):107-118.

45. Manfredi P, Ginste DV, Zutter DD, Canavero FG. Generalized decoupled polynomial chaos for nonlinear circuits with many random parameters. *IEEE Microw Wirel Compon Lett*. 2015;25(8):505-507.

46. Roy DP, Wulder MA, Loveland TR, et al. Landsat-8: science and product vision for terrestrial global change research. *Remote Sens Environ*. 2014;145(5):154-172.

47. Przyborski P, Levy R. “Images,” NASA Earth Observatory, 1999. https://earthobservatory.nasa.gov/images. Accessed March 19, 2020.

48. Ramola A, Shakya AK, Pham DV. Study of statistical methods for texture analysis and their modern evolutions. *Eng Rep*. 2020;2(4):1-24.

49. Permell-Hutton C. The small truth about the big decision: Big vs. Small. RecruitmentXperts Limited, July 4, 2020. https://www.recruitmentxperts.com/xpertcorner/28-06-17/small-truth-about-big-decision-big-vs-small. Accessed August 20, 2020.

---

**How to cite this article:** Shakya AK, Ramola A, Vidyarthi A. Conversion of Landsat 8 multispectral data through modified private content-based image retrieval technique for secure transmission and privacy. *Engineering Reports*. 2020;2:e12273. [https://doi.org/10.1002/eng2.12273](https://doi.org/10.1002/eng2.12273)