IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received January 16, 2021, accepted February 2, 2021, date of publication February 9, 2021, date of current version February 17, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3058112

A Dual Layer Secure Data Encryption and Hiding Scheme for Color Images Using the Three-Dimensional Chaotic Map and Lah Transformation

AMMAR S. ALANAZI
Communication and Information Technology Research Institute, King Abdulaziz City for Science and Technology, Riyadh 11442, Saudi Arabia
e-mail: salanazi@kacst.edu.sa

This work was supported by King Abdulaziz City for Science and Technology.

ABSTRACT The rapid increase in the usage of multimedia content and transmission over the internet demands data securing techniques. In this work, a data encryption technique using a three-dimensional chaotic map and highly nonlinear substitution boxes for the encryption of secret images, followed by a data hiding scheme based on Lah transformation i-e the secret image is first encrypted and then hide in the cover image. For data hiding, integer's polynomial sequence is generated using addition and multiplication in coefficient form by evaluating pixels of images, secret bits of Lah transformed encrypted image are embedded in the LhTs coefficient of cover image partitioned into the cluster of four bits. To ensure minimum distortion coefficient adjustment is done before the embedding process. To obtain the stego image inverse Lah transformation is applied after the embedding process. The security analysis of the proposed dual layer data security scheme is performed, the result shows that the proposed system bearing strong immunity against various cryptographic attacks.

INDEX TERMS Chaotic map, information hiding, Lah transformation, dual layer security.

I. INTRODUCTION

During the communication of digital content over a communication channel, the data is subjected to various security threats. Thus, the privacy protection of digital content during the storage and transmission phase is a critical issue to address. The main procedure used for the privacy protection of digital data is data encryption and data hiding [1], [2]. The encryption process converts the data into a scrambled form that is not understandable by the intruder [3]. The process of hiding secret data into some cover data is known as data hiding [4]. One of the most important characteristics of a good data hiding scheme is the invisibility of the secret data [5]. A lot of research [6], [7] has been carried out in the field of information security [8]–[13]. The work presented in [14] utilizes an improved pixel value order. For homomorphically encrypted images a data hiding scheme is presented in [15] in which part of the secret data can be retrieved into an encrypted domain and the remainder can be extracted after picture decryption. In a single text image, the bit values of certain pixels are reversed into the frame. The preprocessed image is encrypted in the Paillier cryptosystem, with the encrypted image in sequence utilizing two incorporation algorithms. Two enhanced reversible data hiding approaches (RDH) are proposed [16] to not distort the image quality. In applications where the host medium and the secret data are of essential significance, the suggested approaches can be helpful. Approach 1 extends the least significant (LSB) match to the reversibility of dual images. The two photos are the same as the one on the cover. Four identical iterations of the cover illustration are also used in approach 2. Secret information is then encoded in the first couple of identical images with the n-rightest bit replacement (n-RBR) process, while the modified pixel value differencing (MPVD) phase is followed to encrypt the secret data in the last two images. Several multiple reversible data hiding based histograms (MH-RDHs) have recently been proposed [17] to take benefit of the similarities between image contents of diverse texture-characteristics, using some strict laws, e.g., single-character-based sorting monitored by unvarying segmentation of the sorted sequence,

The associate editor coordinating the review of this manuscript and approving it for publication was SK Hafizul Islam.

to create various histograms. This article's [17] clustering algorithm, i.e., Fuzzy C-means (FCM) clustering is used for the creation of numerous histograms. Intensively designed features are used by the FCM to differentiate carriers protected, such as measurement errors, into separate clusters that possess analogous characteristics, which are then utilized in the production of several histograms for the successful embedding of data. In an encrypted image constructed on an adaptive encoding method, a revocable data hiding structure is recommended [18]. To cover the contents of the secret image, on the content-owner side the block permutation along with stream cipher is utilized. The embeddable blocks are first calculated by evaluating the distribution of MSB layers, and the supplementary data is then created by the data hider. To create space for data hiding, the MSB layers of the embeddable blocks are changed to the LSBs. As a result, surplus information can be inserted in encrypted image MSB layers with reversed Huffman code words and auxiliary data. Based on the adaptive encoding method, a reversible data hiding scheme for image encryption is suggested [18]. Block-based permutation and stream cipher enciphering is used to cover the content of the secret image. The analysis of embedded encrypted block MSB layers first generates auxiliary information and then performs the adaptive block encoding based on the MSB and Huffman data hiding code. This helps reversed code words, data support, and extra data to be replaced by reverse Huffman layers to blend into MSB layers of encrypted images. Depending on the accessibility of secret keys for image encryption and data embedding, the receiver can achieve independent data extraction, image decryption, and image recovery operations. A general method for reversible data hiding (MH-RDH) multi histograms and their execution is presented in [19], including calculation sorting of prediction error sequence, the creation of multiple histograms, and the distribution of rates between various histograms. The complexity measurement (CM) focuses on maximizing the relationship in the linear multi-feature combination (MF) and helps to efficiently sort and create multiple histograms. While the problem of the rate allocation between various histograms is developed to increase the rate and the distortion and resolve it by evolutionary algorithms. An encrypted, reversible data hiding system that focuses on the transmission of redundancy is proposed in [20]. MSB-bit planes are replaced by LSB-bit planes at random for each block employing a complex imaging method that can pass redundancy to LSB layers. Blocks and pixels are then scrambled led to further improve security. A sparse compression method that efficiently encodes various types of binary blocks on LSB bit planes can be used to insert additional dataset data into the encrypted LSB image. Based on the available secret keys, the recipient will perform data extraction, file decryption, and image recovery. Data hiding scheme based on the distribution of the discrete cosine transform coefficient is presented in [21]. Different types of images encryption schemes were developed which provides confidentiality to digital contents [22]–[30].

The principal idea of this manuscript is to propose a dual information hiding scheme which not only hide digital content but also provides confidentiality to secret contents which is to be hided in cover medium. The remaining of the article is organized as: section describes the basic concepts utilized in the projected system, Section three is devoted to the proposed encryption and data hiding structure Section four discuss the simulations and results while section five is dedicated to concluding the article.

II. PRELIMINARIES

In this section of the article, some fundamentals of the proposed dual-layer data hiding scheme are being discussed.

A. THREE-DIMENSIONAL CHAOTIC MAP GENERATION

The logistic map as described by Eq. (1) is the simplest way of chaos generation:

$$z_{n+1} = \mu z_n(1 - z_n). \tag{1}$$

To make this equation chaotic the range of initial condition for above map is $z_0 \in (0, 1)$, and $\mu = 4$. The three-dimensional (3D) version of this map is proposed by [24] and is given by Eq. (2-4):

$$x_{n+1} = \mu x_n(1 - x_n) + \alpha y_n^2 z_n + \gamma z_n^3 \tag{2}$$

$$y_{n+1} = \mu y_n(1 - y_n) + \alpha x_n^2 z_n + \gamma x_n^3 \tag{3}$$

$$z_{n+1} = \mu z_n(1 - z_n) + \alpha x_n^2 z_n + \gamma y_n^3 \tag{4}$$

For $3.53 < \mu < 3.81$, $0 < \alpha < 0.022$ and $0 < \gamma < 0.015$ and for initial values of $x, y, z \in [0, 1]$, the above equations exhibit chaotic behavior, the chaos generated by the above three Eqs. (2)–(4) are shown in Fig. 1.

B. ROW AND COLUMN ROTATION

For the image pixels permutations, the proposed algorithm is performed row and column wise rotation first M×N chaotic sequence using Eqs. (5)–(6):

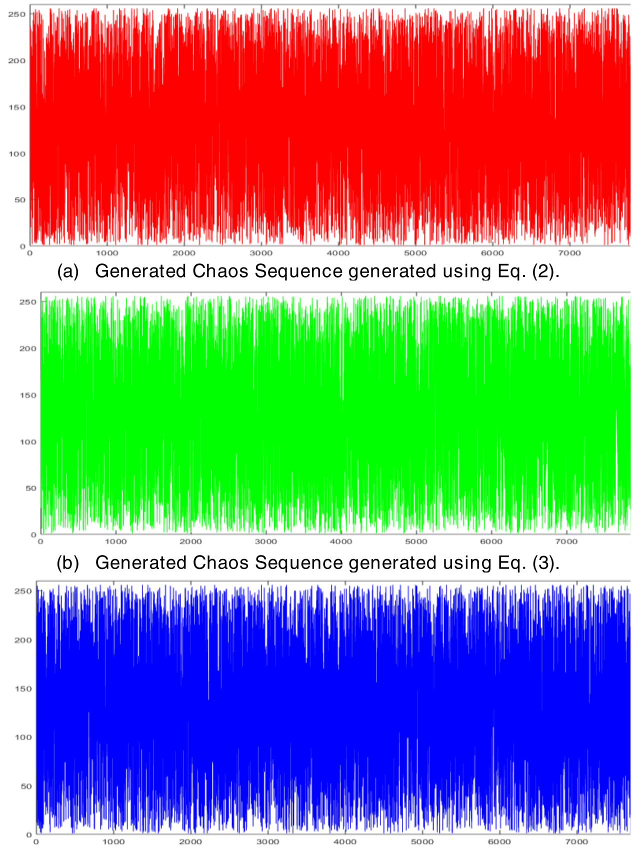
$$x_{n+1} = [(\mu x_n(1 - x_n) + \alpha y_n^2 z_n + \gamma z_n^3) \times 10^8 \mod 256], \tag{5}$$

$$y_{n+1} = [(\mu y_n(1 - y_n) + \alpha x_n^2 z_n + \gamma x_n^3) \times 10^8 \mod 256]. \tag{6}$$

The values of the matrix generated from the above two equations are compared, and the row rotation and column rotation are performed using Eq. (7):

$$pixel\ Permutation = \begin{bmatrix} if\ x_{n+1} < y_{n+1} & Rotate\ Row\ Left \\ if\ x_{n+1} > y_{n+1} & Rotate\ Column\ Left \\ else\ dont\ rotate \end{bmatrix} \tag{7}$$

For decryption, the reverse is done.



(a) Generated Chaos Sequence generated using Eq. (2).

(b) Generated Chaos Sequence generated using Eq. (3).

(c) Generated Chaos Sequence generated using Eq. (4)

FIGURE 1. Generated 3-D Chaos Sequence generated using Eq. (2-4).

C. BLOCK SCRAMBLING

The permuted image is now divided into the blocks and blocks are scrambled using the relation in Eq. (8):

$$Block_{(x,y)} \rightarrow Block_{s(xs,ys)}$$
$$\begin{cases} xs = ((a + D_{\,1,b} + b) \bmod N) + 1, \\ \quad for\ 0\ \le\ a\ \le N - 1 \\ ys = D_{rs,b} \end{cases} \tag{8}$$

For decryption Eq. (9) is used to obtain the image before scrambling of blocks:

$$Block_{s(xs,ys)} \rightarrow Block_{(x,y)}$$
$$\begin{cases} x = ((a - D_{\,1,b} + b) \bmod\ \ N) + 1,\ , \\ \quad for\ 0\ \le\ ia\ \le\ N - 1 \\ y = D_{r,b} \end{cases} \tag{9}$$

whereas $a = x$, and $b = y$, N is the dimensions of the image x and y are the block location in the original image and xs, ys is the new block location in the scrambled image and $D\,(a, b)$ is the 16 × 16 random chaotic scrambling matrix, generated from 3D chaotic map.

D. XOR OPERATION

The permuted and scrambled image is still subjected to attacks based on histogram analysis, now to put immunity against HA attacks, XOR the image with the randomly generated chaotic matrices of the same dimensions that of the original image and then done the phase of substitution using S-boxes.

E. SUBSTITUTION USING CONFUSION COMPONENT

In symmetric-key cryptography, substitution box (S-box) is one of the core elements, used for making the relation between ciphertext and key undetectable. Generally, some number m bits are taken by S-box and transform into some other bits n. S-boxes are normally implemented as lookup tables with 2^{n} words each having n bits. S-boxes do confusion phase of symmetric key cryptography. Confusion implies that each ciphertext of the binary digit (bit) could be based on several parts of the key, obscuring the relation between the two. The ambiguity property hides the cipher-key relationship. This property makes it difficult to find the ciphertext key because if a single bit in the key is changed, it will affect the calculation of the values of some or any of the bits in the ciphertext. The confusion raises the ciphertext ambiguity used by both block and stream ciphers. The proposed dual information hiding mechanism utilized highly nonlinear S-boxes generated by [25].

F. LAH TRANSFORMATION

The transform components $T_0, T_1, T_2, T_{3,} \ldots, T_m$ of b-pixels group $b_0, b_1, \ldots, b_n$ of the encrypted cover image can be computed using the relation in Eq. (10)

$$T_n = \sum_{l=0}^{n} \frac{n!}{l!} \binom{n-1}{n-l} b_k \tag{10}$$

where $0<n<b\text{-}1$. Here image is divided into 4 blocks and do the computations. The Inverse-Lah transformation can be computed using the relation in Eq. (11)

$$b'_k = \sum_{l=0}^{n} \frac{n!}{l!} (-1)^{(n-k)} \binom{n-1}{n-l} s_n \tag{11}$$

G. EMBEDDING PROCESS

First, the encrypted cover image is decomposed into B-pixels groups of non-overlapping blocks and LhT is applied over it. To achieve a high payload of k bits per pixel, mi is the number of bits from the encrypted secret image bitstream is embedded into the i^{th} Lah Transformed coefficients. It is tried with the smaller value of b tried to achieve results in a high payload with acceptable structural similarity. However, for 4 pixels groups of non-overlapping blocks mi can be fabricated as given in Eq. (12):

$$m_i = \left[\begin{array}{ll} k+1 & if\ \ i=0 \\ k-1 & if\ \ i=1 \\ k-1 & if\ \ i=2 \\ k+1 & if\ \ i=3 \end{array} \right. \tag{12}$$

where in the case of the 4 pixels group, the second and third are more sensitive and the first and last are less sensitive against alteration of the coefficient. So fewer bits are embedded in the second and third and more bits are embedded in the first and last pixels. To understand the process better here, let us consider (b_0, b_1, b_2, b_3) with four pixels group of the cover image having values (200, 90, 50, 100) by applying LhT and embedding the bits of the secret encrypted image, we get the values (200, 90, 230, 940) and (206, 91, 230, 939) after coefficient adjustment and inverse Lah transformation, we get (198, 91, 230, 939) and (198, 91, 48, 105). By having a close observation, the cover image pixels (200, 90, 50, 100) are changed into stego image pixels (198, 91, 48, 105), the difference in pixels values are negligible. To obtain the stego image pixels after embedding the inverse Lah Transform is applied. The described process is repeated until all the secret image is embedded and the stego image is obtained.

III. PROPOSED ENCRYPTION AND DATA HIDING SCHEME

The proposed encryption and data hiding scheme comprises the following steps:

Step 1: To start with, parameters for a 3D chaotic map is initialized and three chaotic matrices of the same sizes as the secret image layers are generated.

Step 2: By comparing the values of chaotic matrix X as described in Eq. (5) and Y as described in Eq. (6) row rotation and column rotation are performed using Eq. (7), the reverse can be done for decryption using Eq. (7) but instead of rotating left, rotate right command can be used and comparison of matrix entries start from last and proceeding to the first entry.

Step 3: The resulted image from step 2 is XORed with chaotic matrix z.

Step 4: The processed image resulted from step 3 are divided into blocks and 16 × 16 chaotic scrambling matrix are generated, and scrambling is done using Eq. (8), for decryption the reverse can be done using Eq. (9)

Step 5: The resulted image from step 4 is XORed with chaotic matrix Y, and highly non-linear S-boxes are used for diffusion. At this stage, we have obtained the encrypted version of the secret image as shown in Fig. 3, the process of encryption is shown in Fig. 2. Now the secret image is hided in a cover image.

Step 6: For data hiding, both the secret encrypted image and the cover image are split into respective layers.

Step 7: The images are divided in to block of 4-pixels each and Lah transformation is applied as discussed in section 2.6 of this article.

Step 8: After coefficient adjustment embedding of the encrypted secret image is done in the cover image using the process discussed in section 2.7 of this article.

Step 9: To obtain stego image inverse Lah transformation is applied on every matrix obtain in step 8 and combined as RGB image the stego image is shown in Fig. 3. The procedure for data hiding is shown in Fig. (4).

IV. SIMULATION RESULTS AND SECURITY ANALYSIS

Lena, pepper, baboon, airplane, girl images of size 256 × 256 are utilized in the experimental setup. First, the analysis of the image encryption scheme and then the analysis of the data hiding scheme is presented. For the analysis of image encryption, security performance for secure confidentiality scheme have been discussed in the proceeding sections.

A. STATISTICAL ANALYSIS

To investigate the texture and content of stego, cover image, and encrypted image, statistical analysis is utilized. The statistical analysis can be subcategorized into three groups. The first group relies on the human visual system, the second group of analysis based on correlation amongst the contiguous pixels, and the third category of analysis utilizes the pixels-based measurements. All the analyses are done and displayed in the successive sections.

1) HISTOGRAM ANALYSIS

The histogram is a diagram that describes the number of pixels with each intensity value present in the image. There could be 256 potential intensities for an 8-bit grey image, such that the histogram can graphically represent 256 numbers, showing the pixel distribution of those greyscale values. It is also possible to take color images from histograms-it is possible to take either individual red, green and blue histograms or to create a 3D histogram, each dimension representing a red, blue, and green channel and each pixel point counting brightness. The robustness of encryption and steganographic techniques can be validated by histogram analysis of the secret, encrypted, and stego images. normally the histogram of the plain image is nonuniform as shown in Fig. 5. Apart from other information, this histogram conveys information regarding the brightness, darkness of the image, the histogram of the encrypted image needs to uniform as possible i-e there have to be no variations and the pixels needs to be uniformly distributed in the encrypted image. The histogram of the stego image needs to be similar as possible to the histogram of the cover image for a good data hiding scheme. The detailed histograms of the secret image, secret encrypted image, cover image, and stego image as shown in Fig. (5). The histogram of the encrypted image is uniform as expected and the histogram of the cover image is like the histogram of the stego image.

2) CORRELATION BASED MEASUREMENTS

The pixels in the plain image are highly linearly correlated as shown in Fig. 6. One of the objectives of a good cryptosystem is to minimize the correlation amongst the contiguous pixels and in case of data hiding the correlation amongst the contiguous pixels needs to be linearly correlated as shown in Fig. 6. The correlation coefficient is computed for each layer of the secret image and encrypted image and is displayed in Table 1, less value of CC represents low similarity amongst pixels and the high value of CC represents a strong similarity amongst

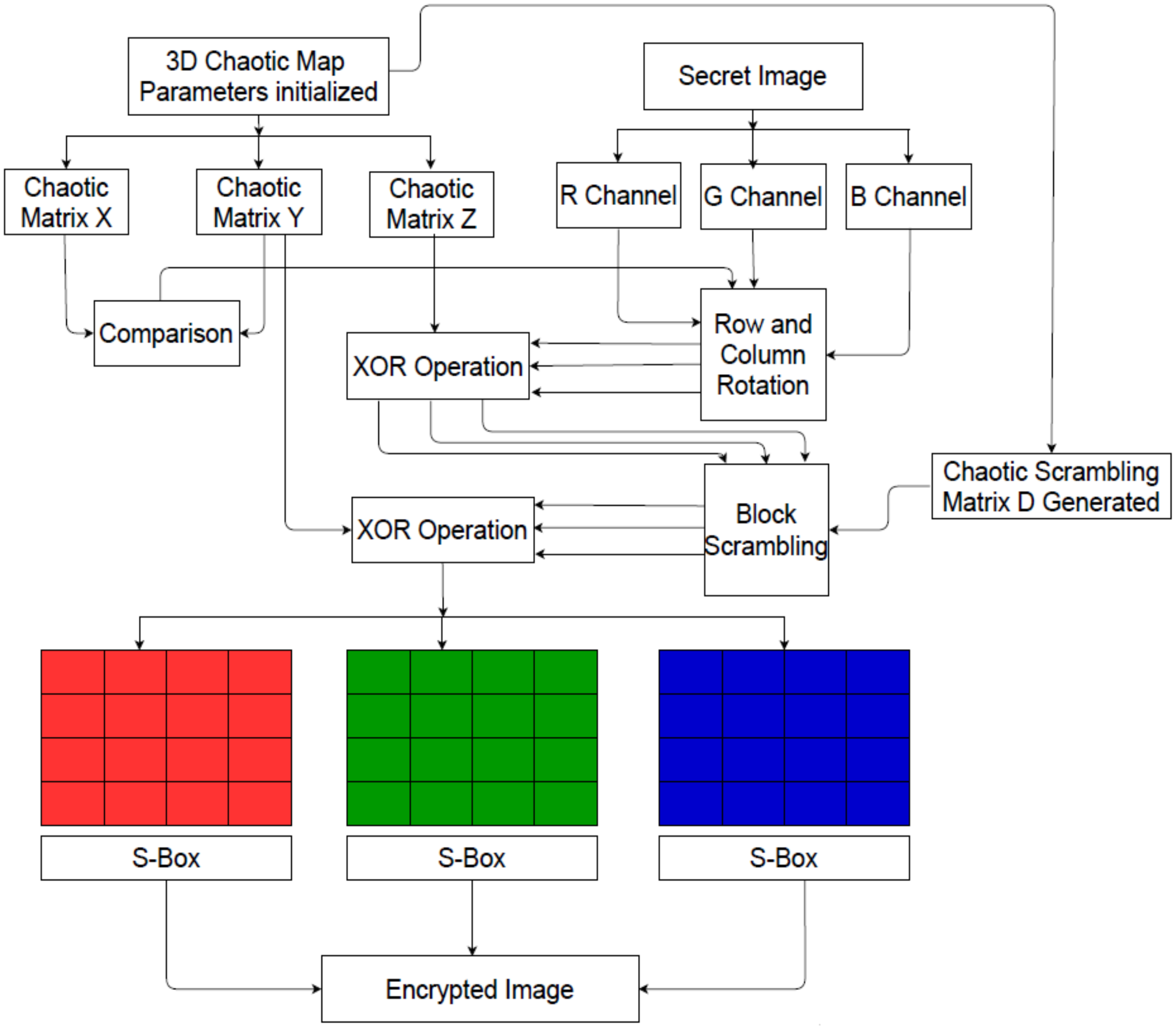


FIGURE 2. Proposed Encryption of the secret image before hiding in the cover image.

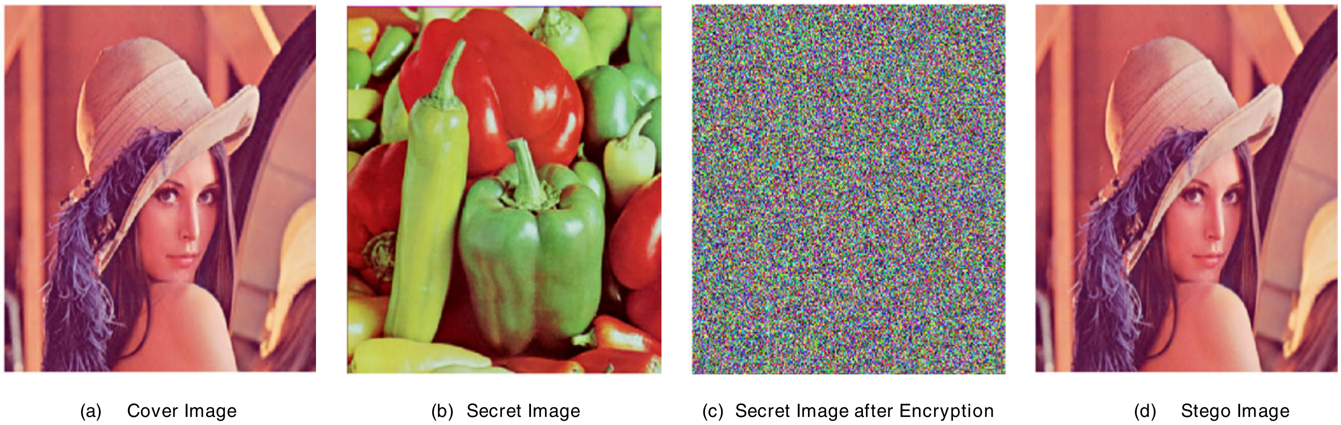

(a) Cover Image (b) Secret Image (c) Secret Image after Encryption (d) Stego Image

FIGURE 3. Original and Processed images.

contiguous pixels. It can be seen from Table 1, that the CC values are nearest to unity in the plain image and the values of the CC are near to zero in the encrypted image also the values of the CC of stego and cover image are approximately

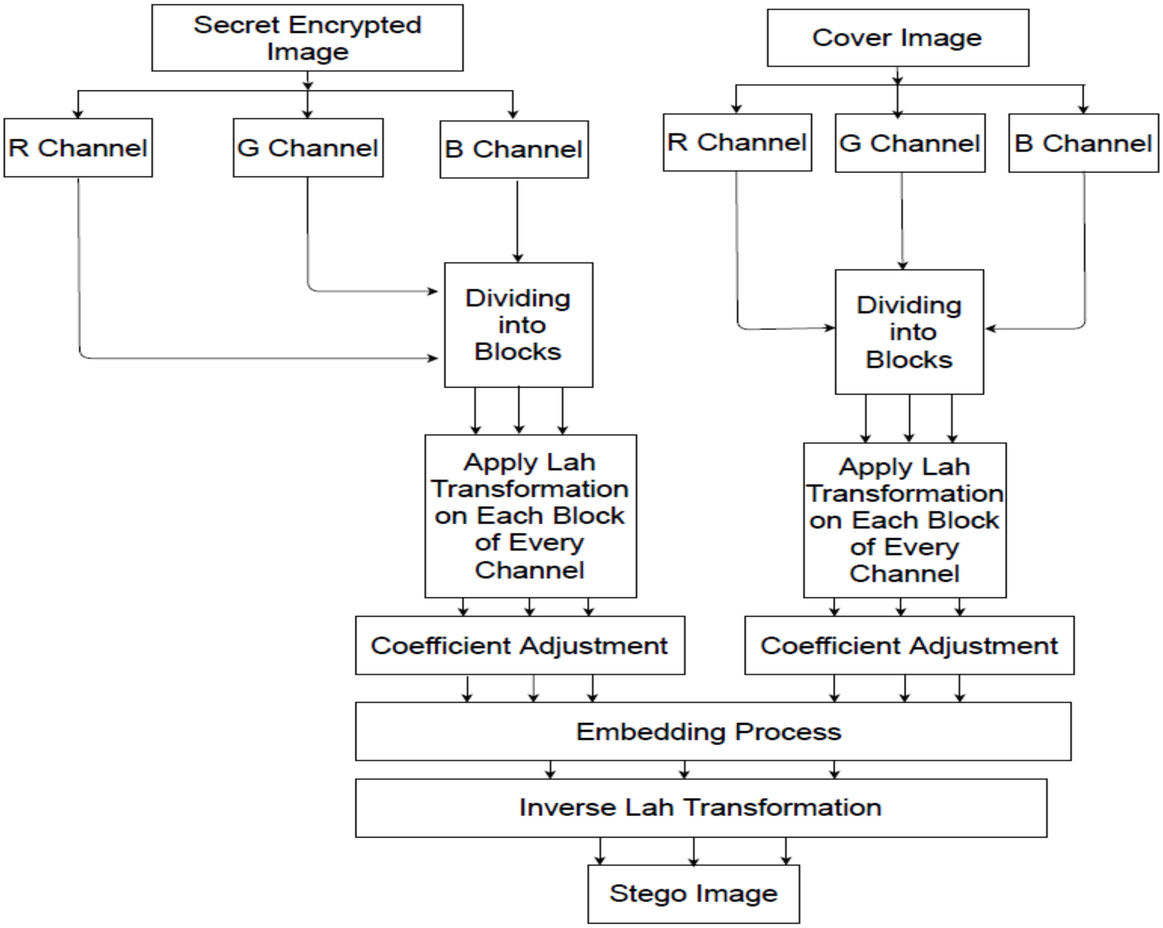
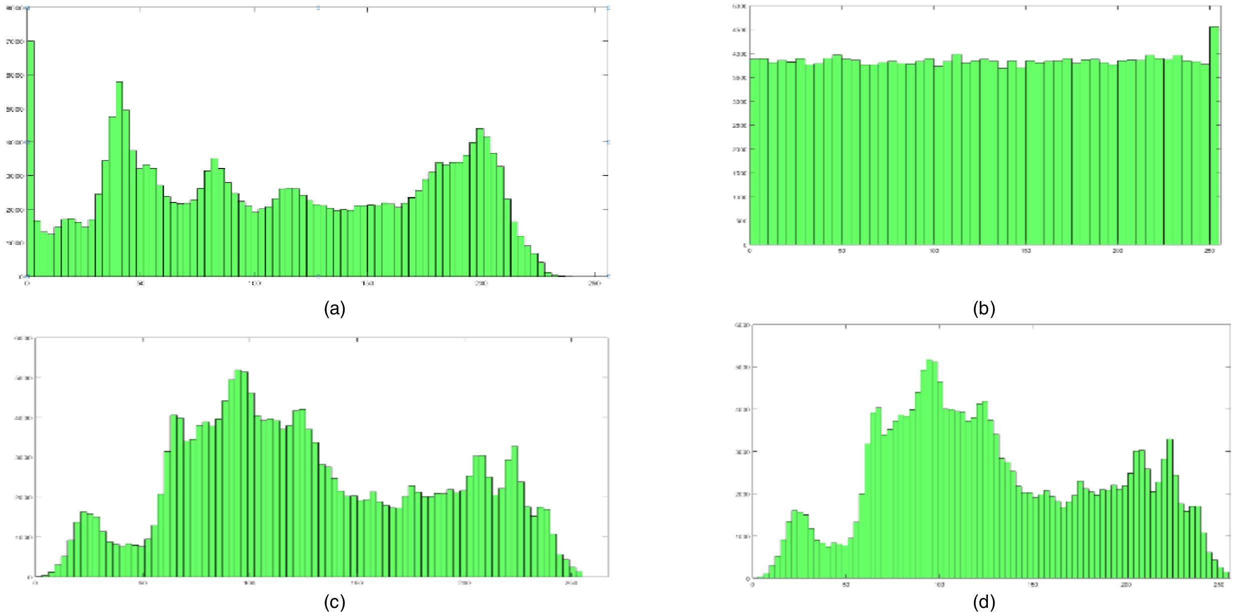


FIGURE 4. Data Hiding Process of Encrypted Secret Image into Cover Image.


(a)

(b)

(c)

(d)

FIGURE 5. Data Hiding Histogram Analysis (a)Histogram of secret image (b) Histogram of the secret image after encryption(c) Histogram of Cover image (d) Histogram of stego image.

similar and close to unity. The correlation-based measurements are further accompanied by the image quality index and its subtests analysis in the proceeding section of the article.

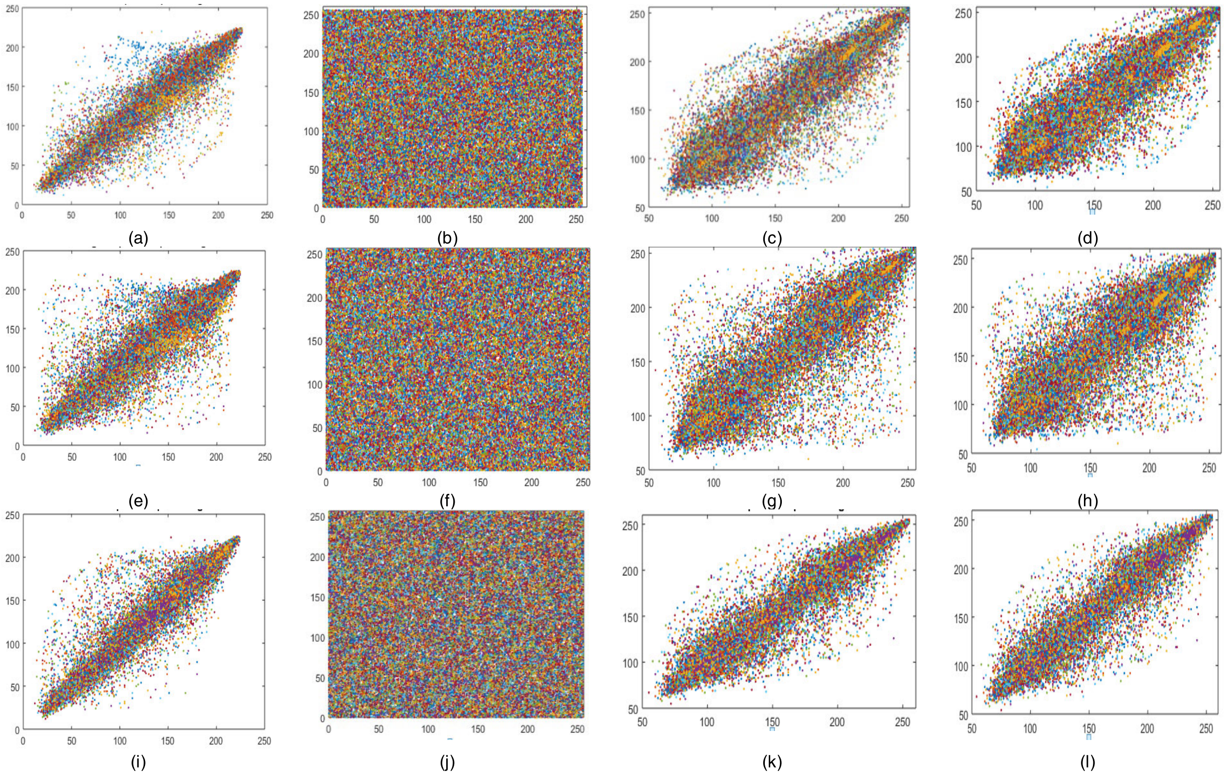


FIGURE 6. (a) Correlation diagram of the secret image in the horizontal direction (b) Correlation diagram of the secret encrypted image in horizontal direction (c) correlation diagram of the cover image in horizontal direction (d) correlation diagram of stego image in the horizontal direction (e) Correlation diagram of the secret image in a diagonal direction (f) Correlation diagram of the secret encrypted image in diagonal direction (g) correlation diagram of the cover image in diagonal direction (h) correlation diagram of stego image in diagonal direction (i) Correlation diagram of the secret image in vertical direction (j) Correlation diagram of the secret encrypted image in vertical direction (k) correlation diagram of the cover image in vertical direction (l) correlation diagram of stego image in the vertical direction.

TABLE 1. IQI Based measurements of secret image, secret encrypted, stego and cover image.

Measurement	The calculated value between cover and stego image			The calculated value between secret and encrypted secret Image		
	R	G	B	R	G	B
Bias	0.0009345	0.0020946	0.0015612	0.2835760	7.1986712	6.1486108
DIV	0.6844292	1.3789877	0.8542886	33.299381	1150.5650	144.35826
CC	0.9499003	0.9716444	0.9683655	0.0064732	0.0058061	0.0058694
Entropy Diff	0.1199681	0.0995761	0.09539906	1.2629468	1.3316288	1.3730162
Local Quality Index Q	0.9582535	0.9792667	0.9747165	0.0004375	-0.000629	-0.001555
RASE	0.5982781	1.3628582	0.9996664	65.524490	864.02227	755.29534
RMSE	0.9952546	0.9912113	0.9822468	88.315574	103.86360	103.75659
SSIM	0.975199	0.9492637	0.972637	0.003146320	0.003028	0.004838485
SC	0.9987	0.9979	0.9977	0.4930	0.2890	0.2910

3) IMAGE QUALITY INDEX (IQI)

To fulfill its function, processed images must be compared with the original image. In addition to visual evaluation, which is mandatory, image quality indices are also very effective in determining which image is more satisfactorily processed (e.g., correlation coefficient, entropy, and so on). The IQI is accompanied by the following measurements. In all the below test O represents the original image and P represents the processed image.

B. BASIS

By utilizing the mean and values of the processed and original image Bais can be computed. The small value of Bais represents strong similarity while a large value of Bais denotes strong dissimilarities. Bias can be computed using the relation in Eq. (12):

$$Bias = 1 - \frac{P}{O}. \tag{13}$$

The values of Bias are computed for each channel of the cover and stego image as well as the secret and encrypted version of the secret image and tabulated in Table 1.

1) CROSS-CORRELATION BASED ANALYSIS (CC)

The resemblance between the two images is quantifying using CC. The range of CC values lies $[-1, 1]$. The -1 shows anti-correlation and 1 shows a strong correlation. The values of the NCC, measured between stego and cover image as well as the secret and encrypted version of the secret image and are displayed in Table 1. CC can be computed using the relation in Eq. (14):

$$CC = \frac{\sigma_{OP}}{\sigma_O \sigma_P}, \tag{14}$$

where σ_{OP} is the covariance and σ_O and, σ_P are the standard deviations of original and processed images.

2) DIFFERENCE IN VARIANCE

The difference in Variance (DIV) are computed using the relation in Eq. (15)

$$DIV = 1 - \frac{\sigma_P^2}{\sigma_O^2} \tag{15}$$

The small value of DIV represents strong similarity while a large value of DIV denotes strong dissimilarities. The values of the DIV, measured between stego and cover image as well as the secret and encrypted version of the secret image and are displayed in Table 1.

3) LOCAL IMAGE QUALITY INDEX (Q)

Local image quality index describes the quality of the processed image and can be computed using the relation in Eq. (16):

$$Q = \frac{4\sigma_{OP}\bar{O}\bar{P}}{(\sigma_O^2 + \sigma_P^2)(\bar{O}^2 + \bar{P}^2)}. \tag{16}$$

The values of image quality index Q have to be interpreted the same as in case of Bias and DIV. The image quality index Q is computed between stego and cover image as well as the secret and encrypted version of the secret image and are displayed in Table 1.

4) RELATIVE AVEREAGE SEPCTRAL ERROR (RASE)

RASE can be computed by utilizing root mean squared error. it gives information regarding the average spectral error. RASE is computed and tabulated in Table 1. The low value of RASE conveys less spectral distortion and the high value of RASE shows high spectral distortion.

5) STRUCTURAL SIMILARITY INDEX (SSIM)

The SSIM can be computed using the relation in Eq. (17)

$$SSIM = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)}, \tag{17}$$

where μ_x, μ_y represents mean of cover and stego images, σ_x^2 and σ_y^2 signifies the variance of cover and stego images and σ_{xy} is covariance of cover and stego images respectively. In our case, SSIM is computed between stego and cover image as well as the secret and encrypted version of the secret image and is displayed in Table 1. The low value of SSIM mean less similarity in structure and a high value of SSIM means high similarity in structure. The values of Q are to be interpreted the same as in case of Bias and DIV. Q is computed between stego and cover image as well as the secret and encrypted version of the secret image and are displayed in Table 1.

6) STRUCTURAL CONTENT

The SC utilizes the analogous section between two images to measure the similarity between two images. In our case, SSIM is computed using relation in Eq. (18), between stego and cover image as well as the secret and encrypted version of the secret image and is displayed in Table 1.

$$SC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(\text{Processed } image(i,j))^2}{\sum_{i=1}^{W}\sum_{j=1}^{H}(Original\ \ image(i,j))^2}. \tag{18}$$

values of Q have to be interpreted the same as in case of Bias and DIV. Q is computed between stego and cover image as well as the secret and encrypted version of the secret image and are displayed in Table 1.

C. PIXEL DIFFERENCE BASED ANALYSIS

In these measurements, the difference between the two-digital content i-e original image and stego image are calculated and their cumulative effect is studied. Usually, the difference is based on pixel difference metrics. This type of measurements includes, average difference (AD), maximum difference (MD), mean squared error (MSE), mean absolute error (MAE), peak signal to noise ratio (PSNR), root mean squared error (RMS) and normalized absolute error (NAE).

1) AVERAGE DIFFERENCE (AD)

The pixel contrast and disparities among the original and processed image can be defined as the AD. The AD measurements for two similar images have to be zero. Mathematically it can be calculated as in Eq. (19)

$$AD = \frac{1}{P \times Q}\sum_{x=1}^{P}\sum_{y=1}^{Q}(P_{x,y} - S_{x,y}), \tag{19}$$

where P and Q are the dimensions of the images, original image P and stego image S and x, y are the respective locations of the pixels. This quantity is widely used in pattern recognition applications. The AD needs to be less for the superior quality of the data hiding scheme. The results are tabulated in Table 2.

2) MAXIMUM DIFFERENCE

The difference between the cover and stego image is referred to as MD.MD can be defined as in Eq. (20)

$$MD = \max(\left|P_{x,y} - S_{x,y}\right|). \tag{20}$$

The measurements of MD between the cover and stego image needs to be low for a good data hiding scheme. The results are tabulated in Table 2.

TABLE 2. Measurements based on pixel difference.

Analysis	The layer of Stego and cover image			
	R	G	B	RGB
MSE	4.736	6.231	6.413	7.711
AD	−0.6324	0.43485	0.261047	0.060378
MD	38	37	39	39

D. ANALYSIS BASED ON INFORMATION THEORY

Analysis based on information entropy is accompanied by Information Entropy, Joint Entropy (JE), Mutual, Relative, and conditional entropy. The computations of these entropies' analysis are as follows:

1) INFORMATION ENTROPY

Let n $\in$ Z and Y $= \{y_1, y_2, y_3, \ldots, y_n\}$ be a set of finite values and having the probability distribution p. The Shanon entropy S(Y) for this finite set (Y, p) can be computed using relation in Eq. (21)

$$S(Y) = \sum_{n \in i} p(i) \log[p(i)], \tag{21}$$

where $p(i)$ represents the probability. For a 256 colors image, the ideal value of entropy is 8. The Information entropy between stego and cover image as well as the secret and encrypted version of the secret image and is computed and displayed in Table (III-IV).

TABLE 3. Analysis based on information theory of cover and stego image.

Information Entropy		RE	MI	CE	JE
Cover	Stego				
7.73300	7.73481	0.000903	6.04178	1.69121	9.42603

TABLE 4. Analysis based on information theory of secret image and encrypted secret image.

Information Entropy		RE	MI	CE	JE
Secret Image	Encrypte d Secret Image				
7.7037542 5	7.999049	3.4215 0	0.23329 7	7.47045 7	15.4695 0

2) JOINT ENTROPY (JE)

The JE among the two images can be computed using the relation in Eq. (22)

$$JE(A, B) = -\sum_{y \in O} \sum_{z \in Pe} p(y, z) \log[p(y, z)], \tag{22}$$

where O and P are the original and Processed Image. The Joint entropy between stego and cover image as well as the secret and encrypted version of the secret image and is computed and displayed in Table (III-IV).

3) CONDITIONAL ENTROPY

The CE among the two images can be computed using the relation in Eq. (23)

$$CE(A/B) = -\sum_{y \in O} \sum_{z \in P} p(O)p(z/y) \log[p(z/y)], \tag{23}$$

The CE between stego and cover image as well as the secret and encrypted version of the secret image and is computed and displayed in Table (III-IV).

4) MUTUAL ENTROPY

The Mutual entropy can be computed by utilizing the JE and CE as depicted in Eq. (24)

$$ME(A, B) = E(A, B) - E(A/B), \tag{24}$$

The ME between stego and cover image as well as the secret and encrypted version of the secret image and is computed and displayed in Table (III-IV).

5) RELATIVE ENTROPY

The RE between stego and cover image as well as the secret and encrypted version of the secret image and is computed and displayed in Tables (III-IV).

TABLE 5. Distance based analysis of stego and cover image.

Analysis	Measurements
Euclidean Distance	1.73758
Mean Squared Euclidean Distance	0.0000153563
Mean Pattern Intensity	0.00955684
Squared Euclidean Distance	3.01918
Correlation Distance	0.000143103
Normalized Squared Euclidean Distance	0.0000715547
Mutual Information Variation	0.361946
Mean Euclidean Distance	0.000000873878
Mean Reciprocal Gradient Distance	0.00103570
Manhattan Distance	432.714
Difference Normalized Entropy	0.182706
Earth Mover Distance	0.000557582
Cosine Distance	0.000024751
Gradient Correlation	0.000518462
Mean Reciprocal Squared Euclidean Distance	0.00103253

E. DISTANCE BASED ANALYSIS OF DATA HIDING SCHEME

In this section of the article, several distance-based analyses of stego and cover images have been performed to validate the dissimilarity of two digital mediums. The low distance represents the strong similarity of stego and cover images. The results of distance-based analysis are tabulated in Table 5.

V. CONCLUSION

In this paper a dual layer security scheme is presented, by utilizing 3D chaotic map and a novel scrambling technique accompanied by high nonlinear S- Boxes the secret image is first encrypted and the by utilizing Lah transformation the encrypted secret image is embedded in the cover image to obtain stego image. The security analysis of both encryption and data hiding scheme is carried out, the results show highly immunity to different types of steganalysis and cryptanalysis attacks.

REFERENCES

[1] N. Alanazi, E. Khan, and A. Gutub, "Efficient security and capacity techniques for arabic text steganography via engaging unicode standard encoding," *Multimedia Tools Appl.*, vol. 80, no. 1, pp. 1403–1431, Jan. 2021.

[2] S. S. Jamal, T. Shah, and I. Hussain, "An efficient scheme for digital watermarking using chaotic map," *Nonlinear Dyn.*, vol. 3, p. 73, Aug. 2013.

[3] U. A. Waqas, M. Khan, and S. I. Batool, "A new watermarking scheme based on daubechies wavelet and chaotic map for quick response code images," *Multimedia Tools Appl.*, vol. 79, nos. 9–10, pp. 6891–6914, Mar. 2020.

[4] Z. Yin, Y. Xiang, and X. Zhang, "Reversible data hiding in encrypted images based on multi-MSB prediction and Huffman coding," *IEEE Trans. Multimedia*, vol. 22, no. 4, pp. 874–884, Apr. 2020.

[5] A. Alghafis, H. M. Waseem, M. Khan, S. S. Jamal, M. Amin, and S. I. Batool, "A novel digital contents privacy scheme based on quantum harmonic oscillator and schrodinger paradox," *Wireless Netw., Internet*, May 2020. [Online]. Available: http://link.springer.com/10.1007/s11276-020-02363-7

[6] S. S. Jamal, M. U. Khan, and T. Shah, "A watermarking technique with chaotic fractional S-Box transformation," *Wireless Pers. Commun.*, vol. 90, no. 4, pp. 2033–2049, Oct. 2016.

[7] S. S. Jamal, S. Farwa, A. H. Alkhaldi, M. Aslam, and M. A. Gondal, "A robust steganographic technique based on improved chaotic-range systems," *Chin. J. Phys.*, vol. 61, pp. 301–309, Oct. 2019.

[8] A. Malik, H. Wang, T. Chen, T. Yang, A. N. Khan, H. Wu, Y. Chen, and Y. Hu, "Reversible data hiding in homomorphically encrypted image using interpolation technique," *J. Inf. Secur. Appl.*, vol. 48, Oct. 2019, Art. no. 102374.

[9] A. K. Sahu and G. Swain, "Dual Stego-imaging based reversible data hiding using improved LSB matching," *Int. J. Intell. Eng. Syst.*, vol. 12, pp. 63–74, Aug. 2019.

[10] J. Qin and F. Huang, "Reversible data hiding based on multiple two-dimensional histograms modification," *IEEE Signal Process. Lett.*, vol. 26, no. 6, pp. 843–847, Jun. 2019.

[11] S. S. Jamal, T. Shah, S. Farwa, and M. U. Khan, "A new technique of frequency domain watermarking based on a local ring," *Wireless Netw.*, vol. 25, no. 4, pp. 1491–1503, May 2019.

[12] H. M. Waseem and M. Khan, "A new approach to digital content privacy using quantum spin and finite-state machine," *Appl. Phys. B, Lasers Opt.*, vol. 125, no. 2, p. 27, Feb. 2019.

[13] A. Alghafis, H. M. Waseem, M. Khan, and S. S. Jamal, "A hybrid cryptosystem for digital contents confidentiality based on rotation of quantum spin states," *Phys. A, Stat. Mech. Appl.*, vol. 554, Sep. 2020, Art. no. 123908.

[14] S. Weng, Y. Shi, W. Hong, and Y. Yao, "Dynamic improved pixel value ordering reversible data hiding," *Inf. Sci.*, vol. 489, pp. 136–154, Jul. 2019.

[15] H.-T. Wu, Y.-M. Cheung, Z. Yang, and S. Tang, "A high-capacity reversible data hiding method for homomorphic encrypted images," *J. Vis. Commun. Image Represent.*, vol. 62, pp. 87–96, Jul. 2019.

[16] A. K. Sahu and G. Swain, "High fidelity based reversible data hiding using modified LSB matching and pixel difference," *J. King Saud Univ.—Comput. Inf. Sci., Internet*, Jul. 2019. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S1319157819304124

[17] J. Wang, N. Mao, X. Chen, J. Ni, C. Wang, and Y. Shi, "Multiple histograms based reversible data hiding by using FCM clustering," *Signal Process.*, vol. 159, pp. 193–203, Jun. 2019.

[18] Y. Fu, P. Kong, H. Yao, Z. Tang, and C. Qin, "Effective reversible data hiding in encrypted image with adaptive encoding strategy," *Inf. Sci.*, vol. 494, pp. 21–36, Aug. 2019.

[19] J. Wang, X. Chen, J. Ni, N. Mao, and Y. Shi, "Multiple histograms-based reversible data hiding: Framework and realization," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 30, no. 8, pp. 2313–2328, Aug. 2020.

[20] C. Qin, X. Qian, W. Hong, and X. Zhang, "An efficient coding scheme for reversible data hiding in encrypted image with redundancy transfer," *Inf. Sci.*, vol. 487, pp. 176–192, Jun. 2019.

[21] Y. Li, S. Yao, K. Yang, Y.-A. Tan, and Q. Zhang, "A high-imperceptibility and histogram-shifting data hiding scheme for JPEG images," *IEEE Access*, vol. 7, pp. 73573–73582, 2019.

[22] E. Gao, Z. Pan, and X. Gao, "Reversible data hiding based on novel pairwise PVO and annular merging strategy," *Inf. Sci.*, vol. 505, pp. 549–561, Dec. 2019.

[23] T. Unkašević, Z. Banjac, and M. Milosavljević, "A generic model of the pseudo-random generator based on permutations suitable for security solutions in computationally-constrained environments," *Sensors*, vol. 19, no. 23, p. 5322, Dec. 2019.

[24] P. N. Khade and M. Narnaware, "3D Chaotic Functions for Image Encryption," *IJCSI Int. J. Comput. Sci.*, vol. 9, no. 3, pp. 323–328, 2012.

[25] K. M. Ali and M. Khan, "A new construction of confusion component of block ciphers," *Multimedia Tools Appl.*, vol. 78, no. 22, pp. 32585–32604, Nov. 2019.

[26] A. Alghafis, N. Munir, M. Khan, and I. Hussain, "An encryption scheme based on discrete quantum map and continuous chaotic system," *Int. J. Theor. Phys.*, vol. 59, no. 4, pp. 1227–1240, Apr. 2020.

[27] S. I. Batool, T. Shah, and M. Khan, "A color image watermarking scheme based on affine transformation and S 4 permutation," *Neural Comput. Appl.*, vol. 25, nos. 7–8, pp. 2037–2045, Dec. 2014.

[28] M. Khan, S. S. Jamal, and U. A. Waqas, "A novel combination of information hiding and confidentiality scheme," *Multimedia Tools Appl.*, vol. 79, pp. 30983–31005, Nov. 2020, doi: 10.1007/s11042-020-09610-1.

[29] M. Khan and Z. Asghar, "A novel construction of substitution box for image encryption applications with gingerbreadman chaotic map and s8 permutation," *Neural Comput. Appl.*, vol. 29, no. 4, pp. 993–999, Feb. 2018.

[30] S. Tariq, M. Khan, A. Alghafis, and M. Amin, "A novel hybrid encryption scheme based on chaotic Lorenz system and logarithmic key generation," *Multimedia Tools Appl.*, vol. 79, no. 31, pp. 23507–23529, 2020.

AMMAR S. ALANAZI received the bachelor's degree in computer science from King Saud University, the master's degree in information technology from the University of New South Wales Sydney with a specializing in artificial intelligence and database systems, and the Ph.D. degree in computer science from the University of New South Wales Sydney. He is currently the Director of the National Center for Transport Technology and Logistic Services, King Abdulaziz City for Science and Technology (KACST). His research interests include artificial intelligence, machine learning and data mining, intelligent transport systems, secure communications, and blockchains.