A DNA Based Colour Image Encryption Scheme Using A Convolutional Autoencoder

FAWAD AHMED, Pakistan Navy Engineering College, NUST, Pakistan

MUNEEB UR REHMAN, HITEC University, Pakistan

JAWAD AHMAD, School of Computing, Edinburgh Napier University, United Kingdom

MUHAMMAD SHAHBAZ KHAN, HITEC University, Pakistan

WADII BOULILA, Prince Sultan University, Saudi Arabia and University of Manouba, Tunisia

GAUTAM SRIVASTAVA, Brandon University, Canada, China Medical University, Taiwan, and Lebanese American University, Lebanon

JERRY CHUN-WEI LIN, Western Norway University of Applied Sciences, Norway

WILLIAM J. BUCHANAN, School of Computing, Edinburgh Napier University, United Kingdom

With the advancement in technology, digital images can easily be transmitted and stored over the Internet. Encryption is used to avoid illegal interception of digital images. Encrypting large-sized colour images in their original dimension generally results in low encryption/decryption speed along with exerting a burden on the limited bandwidth of the transmission channel. To address the aforementioned issues, a new encryption scheme for colour images employing convolutional autoencoder, DNA and chaos is presented in this paper. The proposed scheme has two main modules, the dimensionality conversion module using the proposed convolutional autoencoder, and the encryption/decryption module using DNA and chaos. The dimension of the input colour image is first reduced from $N \times M \times 3$ to $P \times Q$ gray-scale image using the encoder. Encryption and decryption are then performed in the reduced dimension space. The decrypted gray-scale image is upsampled to obtain the original colour image having dimension $N \times M \times 3$. The training and validation accuracy of the proposed autoencoder is 97% and 95%, respectively. Once the autoencoder is trained, it can be used to reduce and subsequently increase the dimension of any arbitrary input colour image. The efficacy of the designed autoencoder has been demonstrated by the successful reconstruction of the compressed image into the original colour image with negligible perceptual distortion. The second major contribution presented in this paper is an image encryption scheme using DNA along with multiple chaotic sequences and substitution boxes. The security of the proposed image encryption algorithm has been gauged using several evaluation parameters, such as histogram of the cipher image, entropy, NPCR, UACI, key sensitivity, contrast, etc. The experimental results of the proposed scheme demonstrate its effectiveness to perform colour image encryption.

CCS Concepts: • **Security and privacy → Cryptography, DNA encoding, S-box Substitution, Chaotic maps**; • **Computing methodologies → Convolutional AutoEncoder**.

Additional Key Words and Phrases: autoencoder, chaos, DNA coding, deep learning, colour image encryption, dimensionality reduction
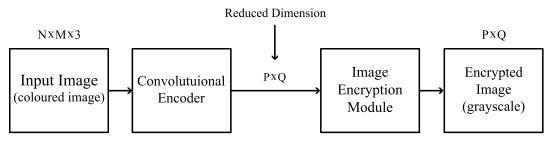
Authors' addresses: Fawad Ahmed, fawad@pnec.nust.edu.pk, Department of Cyber Security, Pakistan Navy Engineering College, NUST, Karachi, Pakistan, 75350; Muneeb Ur Rehman, muneeb95rehman@gmail.com, Department of Electrical Engineering, HITEC University, Taxila, Pakistan; Jawad Ahmad, School of Computing, Edinburgh Napier University, Edinburgh, United Kingdom; Muhammad Shahbaz Khan, shahbaz.khan@hitecuni.edu.pk, Department of Electrical Engineering, HITEC University, Taxila, Pakistan, 47080; Wadii Boulila, wboulila@psu.edu.sa, Robotics and Internet-of-Things Laboratory, Prince Sultan University, Riyadh, Saudi Arabia, RIADI Laboratory and University of Manouba, Manouba, Tunisia; Gautam Srivastava, srivastavag@brandonu.ca, Math and Computer Science, Brandon University, Brandon, Canada, Research Centre for Interneural Computing and China Medical University, Taichung, Taiwan , Dept of Computer Science and Math and Lebanese American University, Beirut, Lebanon; Jerry Chun-Wei Lin, jerrylin@ieee.org, Western Norway University of Applied Sciences, Bergen, Norway; William J. Buchanan, B.Buchanan@napier.ac.uk, School of Computing, Edinburgh Napier University, Edinburgh, United Kingdom.

1 INTRODUCTION

Due to advancements in network communication, the Internet of Things (IoT), telemedicine, online biometric systems, and social media, a large amount of digital images are transmitted over the Internet. The information contained in these digital images can be illegally intercepted and tampered during the transmission or storage process. Hence, there is an indispensable need to secure the transmission and storage of digital images, and in this context, image encryption plays a vital role [24]. Various encryption schemes, such as, DES, 3DES, AES, RSA, etc., are most commonly used for securing digital data over open networks. But it is pertinent to mention here that the data pattern in images is entirely different from the text data. Images contain a large number of pixels , and they have a high degree of correlation between their adjacent pixels [25]. Due to this reason, securing image data is more complex than the text data and hence, the aforementioned text-based encryption schemes are often unsuitable for image encryption [39]. Moreover, for the high definition (HD) colored images, these conventional encryption schemes involve extra operations, which result in increased computational time and power. Consequently, these schemes exhibit low encryption and decryption speeds that may lead to significant delays in real-time communication. In recent years, there has been a surge in the number of image encryption schemes proposed in the literature. The application of chaos theory and DNA sequencing in image encryption has proved to be quite effective and efficient in securing digital images [10, 36, 45, 51]. Therefore, the main motivation of this paper was to develop a chaos and DNA-based image encryption scheme, specifically for HD-colored images that should not only be highly secure but should also address the latency issues faced during the encryption and transmission processes.

The chaotic maps possess several interesting properties such as pseudo-randomness, unpredictability, mixing (ergodicity), and high sensitivity due to change in control parameters and initial conditions [10, 25, 30, 51]. In addition to these properties, chaotic maps also have reduced mathematical complexity and a higher level of security. DNA computing, on the other hand, involves utilization of DNA coding sequences for carrying and securing digital information [28]. These coding sequences are generated by using four types of DNA nucleotide bases, i.e., A, C, G and T. DNA computing performs exceptionally well when dealing with large data and parallelism, resulting in reduced computational power during the transmission of digital information. DNA coding in conjunction with chaotic maps has opened a new paradigm of image encryption [31, 48, 49] and hence, needs to be properly explored to propose more secure and highly efficient encryption schemes.

As described previously, the image data is quite large as compared to text data. Therefore, storing and transmitting such a large amount of data (especially HD colored images) is quite challenging. In addition to increasing the computational complexity of the encryption algorithm, it also increases the bandwidth requirement of the transmission channel as well. This makes it difficult to apply complex image encryption algorithms on large-size colored images in real-time. For better encryption and decryption speeds, recent literature reveals that the deep neural networks based autoencoders [22] exhibit promising results. Such schemes are based on the encoder-decoder paradigm for dimensionality reduction, which helps to decrease the computational complexity of the encryption algorithm. Autoencoders solve the latency issues by first reducing the dimension of the input colour image and then applying the encryption algorithm in the reduced dimension space. Due to less number of pixels in the reduced dimension space, it becomes comparatively easy to practically implement complex image encryption algorithms on edge devices. Thus, the motivation to use an autoencoder-based encryption scheme is to achieve real-time secure image transmission/storage without exerting a burden on the available bandwidth, especially on edge devices in IoT [26].

Reduced Dimension

NxMx3

| Input Image (coloured image) | → | Convolutuional Encoder | PxQ → | Image Encryption Module | → | Encrypted Image (grayscale) |

PxQ

where P, Q < N, M

Fig. 1. Basic Workflow of Image Encryption.

Decrypted Image

PxQ

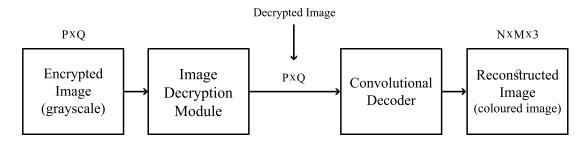| Encrypted Image (grayscale) | → | Image Decryption Module | PxQ → | Convolutional Decoder | → | Reconstructed Image (coloured image) |

NxMx3

Fig. 2. Basic Workflow of Image Decryption.

Various DNA-based encryption schemes can be found in the literature that exhibits slow encryption and decryption schemes. Despite being secure enough, these schemes cannot be implemented in real-time on today's small-size IoT devices. For instance, the first method to use DNA computing for data encryption was the Hiding Messages in Microdots [13] scheme, but it was extremely slow. Even some of the recent and novel techniques, such as the Public Key System by using DNA (PKSDNA) [43], the Chaos-Based Image Encryption (CBIE) [17], the DNA-based Reversible Data Hiding Scheme (RDHS) [44], and the Double-Layer Data Hiding scheme (DLDH) [47] pose latency issues. These schemes take a lot of time for encrypting and decrypting multimedia files, and also while generating or retrieve secret keys.

To solve the aforementioned problems of existing schemes, this paper presents a new autoencoder based image encryption scheme for large size colored images. The proposed scheme consists of two modules; 1) A deep learning-based convolutional autoencoder for dimensionality reduction module, and 2) A Chaos and DNA-based image encryption module.The basic workflow of the proposed image encryption and decryption modules is given in Fig. 1 and Fig. 2, respectively. A colour image having a dimension of N×M×3 is first compressed to a lower dimension P×Q using the proposed convolutional autoencoder model. Encryption is performed in the compressed domain. The encrypted image is then decrypted using the decryption module to retrieve back the plaintext image of dimension $P \times Q$. This decrypted image is then given to the decoder to get back the original colour image of dimension $N \times M \times 3$. It is pertinent to mention that the proposed autoencoder is designed to reconstruct the original colour image with negligible perceptual distortion as evident from the results presented in the paper.

Following are the important contributions of this work:

3

- A convolution autoencoder is proposed to reduce the dimension of the input colour image.
- A new image encryption technique is proposed that uses DNA, chaos, and multiple s-boxes to effectively encrypt and decrypt images in lower dimension space.
- Due to the utilization of multi-chaotic maps, the proposed scheme has a significantly higher keyspace when compared with other schemes.

The remaining sections are structured as follows. Recent literature covering image encryption schemes that use chaos, chaos+DNA, and deep learning is presented in Section 2. Important details related to the chaotic maps used in this paper are discussed in Section 3. In Section 4, the proposed image encryption scheme is presented. Section 5 contains experimental results depicting the quality of reconstructed images and the encryption algorithm, thus proving the effectiveness of the proposed scheme. Finally, Section 6 presents conclusion and future directions.

2 RELATED WORK

In the literature, several encryption schemes for images employing chaotic maps have been proposed [32, 33, 37]. Chaotic maps are used due to their inherent properties, such as unpredictability, pseudo-randomness, high sensitivity for control parameters and initial conditions, and mainly ergodicity. For example, various architectures using chaos to permute and diffuse digital images are presented in [20]. Similarly for video encryption, a chaos-based scheme is presented in [2] that uses the inherent property of the HEVC standard to achieve improved security and exhibit secure real-time video encryption with an optimal bit rate. In addition, chaos with multi-dimensional feature vectors has also been utilized in improving the security of steganographic approaches [7]. The results show that irrespective of the size of the message, the presented steganalysis system can effectively detect hidden information. Furthermore, a neural network based on chaos having key dependent hash functions is presented in [1]. Pseudo-chaotic samples have been generated that are fed into the neural structure as parameter values. The presented architecture helps in generating hash functions having good statistical features along with high message and key sensitivity. Moreover, the effectiveness of chaotic functions against cryptanalysis has been analyzed in [14]. For this purpose, various s-boxes have been designed by using two heuristic methods. The designed s-boxes exhibit exceptional results when compared to other s-boxes available in the literature.

Moreover, in the last few years, chaos-based encryption has been utilized in conjunction with DNA computing to devise new image encryption schemes [10, 51, 52]. DNA computing is the application of various biological and algebraic processes applied to DNA sequences, e.g., addition, XOR and subtraction operations on DNA coded sequences. These operations are recently being preferred to be used with chaos-based encryption schemes, for example, an image encryption algorithm based on a compound chaotic map and varying DNA coding is presented in [50]. The proposed algorithm executes effectively in terms of security performance and can be compared with already available chaos-based encryption schemes. Similarly, another image encryption algorithm is presented in [46] that combines a 1D logistic map, DNA coding, and multi-objective particle swarm optimization (MOPSO). The presented results exhibit resistance of the proposed algorithm against several attacks along with excellent entropy and correlation-coefficient of the ciphertext. Apart from 1D chaotic systems, a 3D chaotic system has also been used with DNA coding in [23]. The presented encryption scheme utilizes all 24 rules of DNA coding with 16 joint operations that make this scheme resistant to several attacks and an excellent scheme for securing digital images. Furthermore, DNA encryption and chaos have also been utilized for the encryption of coloured images [9]. This scheme utilizes permutation by shuffling the RGB components of the input colour image. The permuted components are then recombined by DNA encoding, and finally,

diffusion is used on the encoded DNA matrix. DNA encryption schemes are also being preferred for cloud environments [34], [35], [41]. In [34] DNA computing is used for generating a 1024-bit secret key, and a DNA reference key for better security. Similarly, in [35] for a key generation the DNA computing has been combined with user attributes and the MAC address of the user for improved security. DNA computing-based multifold symmetric key encryption scheme has been presented in [41] which encrypts data before uploading it to the cloud. DNA computing also plays a potential role in securing medical images in smart healthcare systems [5, 8, 12, 18].

In addition to chaos and DNA encryption, deep learning has recently been playing a potential role in image encryption. Most of the presented techniques utilize the encoder-decoder approach. Autoencoders are extensively being utilized for dimensionality reduction and to increase the networks' performance. Recently, various stacked autoencoders and convolutional autoencoders have been explored and designed for encryption/decryption purposes, for example, a stacked autoencoder based on a multi-layer model for compression and encryption of images has been presented in [21]. The first layer of the model compresses the input image. The compressed image is then encrypted using a chaotic logistic map. Such models hold importance in applications where transmission speed is also as important as the security of the images. Similarly, another framework utilizes a neural network-based encoder and decoder for encryption and decryption, respectively [19]. The presented framework is targeted for lossy encryption and decryption and exhibits adequate performance where exact reconstruction of the input image is not a strict requirement.

Majority of the image encryption schemes available in the literature, including the ones discussed above have latency problems in case encryption and decryption of large-size images are required. This problem becomes more pronounced when the input image is a colour image. In such a case, there are three colour planes, thus increasing the size of the images by three times. Although several autoencoders can be found in literature, however, the reconstructed image quality is not very high. Moreover, most of the autoencoders available in the literature have been designed for low to medium size digital images. To address the aforementioned problem, the proposed scheme uses a new autoencoder design to effectively reduce the dimension of the input image from $N \times M \times 3$ to $P \times Q$. Thus a colour image is converted by the autoencoder into a grayscale image. For example, in this paper, the input colour images used have dimensions $512 \times 768 \times 3$ pixels. The autoencoder converts the input colour image to a gray-scale image having dimension 384×512 pixels. Encryption and decryption are then performed in the reduced dimension space using a new DNA-based technique employing multiple chaotic sequences and substitution boxes to make the cipher image random, as evident from the results presented in the paper.

3 PRELIMINARIES

3.1 Utilized Chaotic Maps

There are two broad categories of chaotic systems: one-dimensional and multi-dimensional. Unlike multi-dimensional, one-dimensional chaotic systems such as logistic maps etc., are straightforward to implement. However, there are drawbacks of one-dimensional maps that include their susceptibility to high correlation, as well as their restricted or discontinuous chaotic range and high probability of uniform data distribution in the output chaotic sequence. Thus, in this work, we have used four multi-dimensional maps due to low correlation, higher keyspace and non-uniform data distribution.

Four different chaotic maps are used in this work to introduce randomness at different stages of the encryption process. The four chaotic maps are the TD-ERCS map, the Intertwining map, the Chirikov map, and the NCA map. A

brief description of these maps is as follows:

TD-ERCS Map

The TD-ERCS map is a two-dimension chaotic system proposed in the year 2004 and further developed to exhibit a large domain, zero correlation and a stable probability distribution [27]. In this work, the TD-ERCS map is used for random permutation of pixel values. The TD-ERCS map is expressed as:

$$
\begin{cases}
x_n = -\dfrac{2k_{n-1}y_{n-1}+x_{n-1}(\mu^2-k_{n-1}^2)}{\mu^2+k_{n-1}^2} \\
y_n = k_{n-1}(x_n - x_{n-1}) + y_{n-1}, \quad n = 1, 2, 3...
\end{cases}
\tag{1}
$$

where

$$
k_n = \frac{2k'_{n-m} - k_{n-1} + k_{n-1}(k'_{n-m})^2}{1 + 2k_{n-1}k'_{n-m} - k(k'_{n-m})^2}
$$

$$
k'_{n-m} =
\begin{cases}
-\dfrac{x_{n-1}}{y_{n-1}}\mu^2 & n < m \\
-\dfrac{x_{n-m}}{y_{n-m}}\mu^2 & n \geq m
\end{cases}
$$

$$
y_0 = \mu\sqrt{1 - x_0^2}
$$

$$
k'_0 = -\frac{x_0}{y_0}\mu^2
$$

$$
k_0 = -\frac{\tan\alpha + k'_0}{1 - k'_0\tan\alpha}
$$

$$
\begin{cases}
\mu \in (0, 1) \\
x_0 \in [-1, 1] \\
\alpha \in (0, \pi) \\
m = 2, 3, 4, 5...
\end{cases}
$$

In the above equation, μ, x_0, α and m are called the initial parameters. As outlined in our previous work [3], the TD-ERCS map holds the property of being sensitive to the initial conditions and ergodicity and hence can be effectively used for image encryption.

Intertwining Map

The intertwining map is used for random matrix generation and is written as [4]:

$$
\begin{cases}
X_{n+1} = (\lambda \times A_1 \times Y_n \times (1 - X_n) + Z_n)mod(1), \\
Y_{n+1} = (\dfrac{\lambda \times A_2 \times Y_n + Z_n}{1+(X_{n+1})^2})mod(1), \\
Z_{n+1} = (\lambda \times (X_{n+1} + Y_{n+1} + A_3) \times sin(Z_n)mod(1).
\end{cases}
\tag{2}
$$

where X_n, Y_n and $Z_n \in (0, 1)$, $0 \leq \lambda \leq 3.999$, $|A_1| > 33.5$, $|A_2| > 37.9$, $|A_3| > 35.7$.

Chirikov Map

The Chirikov map is used to randomly select the DNA coding rules. Its mathematical model is as follows [15]:

$$A_{n+1} = (A_n + B_n) \bmod (N),\qquad(3)$$

$$B_{n+1} = (A_n + \eta \times \mathrm{Sin}(\frac{2\pi A_n}{N})) \bmod (N),\qquad(4)$$

where N is the height/width of a square image, $\eta > 0$ and is used as a control parameter for the secret key, A_n and B_n are real numbers whose range is between 0 to N.

NCA Map

The Nonlinear Chaotic Algorithm (NCA) is employed for randomly selecting one of the three S-boxes. These S-boxes are discussed in our previous work [38]. The NCA map is expressed as [4]:

$$C_{n+1} = (1 - \xi^{-4}).\cot(\frac{\chi}{1+\xi}).(1 + \frac{1}{\xi})^{\xi}.\tan(\chi C_n).(1 - C_n)^{\xi},\qquad(5)$$

where the seed parameters are:

$$\begin{cases} C_n \in (0,1) \\ \chi \in (0,1.4] \\ \xi \in [5,43] \\ \text{or} \\ C_n \in (0,1) \\ \chi \in (1.4,1.5] \\ \xi \in [9,38] \\ \text{or} \\ C_n \in (0,1) \\ \chi \in (1.5,1.57] \\ \xi \in [3,15] \end{cases}$$

3.2 DNA Coding

Adenine (A), cytosine (C), guanine (G) and thymine are the nucleic bases to generate different DNA sequences. The nucleic bases, 'adenine and thymine ' and 'guanine and cytosine' are complements of each other. In the proposed encryption scheme, the aforementioned DNA nucleic bases A, T, G and C are represented by the binary codes 00, 01, 10, and 11, respectively. Hence, 24 different coding sequences can be produced. However, the binary codes '00 and 11', and '01 and 10' are complements of each other and hence, only 8 out of 24 coding rules satisfy the complementary criterion for the four bases. The 8 rules for DNA coding are shown in Table 1 [49]. Furthermore, each pixel of a gray-scale image is represented by a value between 0 and 255. The binary representation of a pixel value can be divided into 4 groups, each group made up of two bits. The two bits of each group can then be represented using the DNA basis, depending on the selected rule. As an example, a pixel having a value of '200' can be represented in binary as '11001000', and by following the R2 rule given in Table 1 [49], the DNA sequence for this pixel is 'TACA'. DNA decoding can be performed similarly by following the appropriate rule.

Table 1. The Eight DNA rules with binary coding.

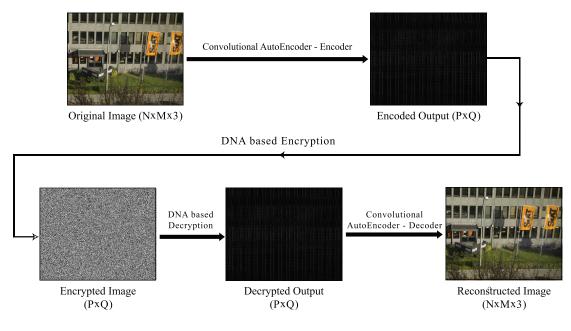| Code	R1	R2	R3	R4	R5	R6	R7	R8
00	[A]	[A]	[C]	[C]	[G]	[G]	[T]	[T]
01	[C]	[G]	[A]	[T]	[A]	[T]	[C]	[G]
10	[G]	[C]	[T]	[A]	[T]	[A]	[G]	[C]
11	[T]	[T]	[G]	[G]	[C]	[C]	[A]	[A]

Fig. 3. A Pictorial Flow Depicting the Workflow of the Proposed Scheme.

4 THE PROPOSED METHODOLOGY

The proposed scheme consists of two main parts, the Convolution Autoencoder-based dimensionality reduction module, and the DNA-based image encryption module. A colour input image of size $N \times M \times 3$ is first reduced to a lower dimension gray-scale image of size $P \times Q$ after passing through a trained convolution-based encoder model. The cipher image is obtained by applying the encryption algorithm on the $P \times Q$ gray-scale image. The encrypted image is then decrypted using the decryption module and subsequently decompressed using upsampling by the decoder to retrieve the original colour image with negligible loss of information. Figure 3 shows the workflow of the proposed colour image encryption scheme and Fig. 4 shows the detailed architecture of the proposed autoencoder illustrating the encoder, decoder along with the encryption and decryption modules. The Kodak dataset[1] has been used in this paper for both the dimensionality reduction module and the encryption module. The next section presents details about the proposed autoencoder module for dimensionality reduction.
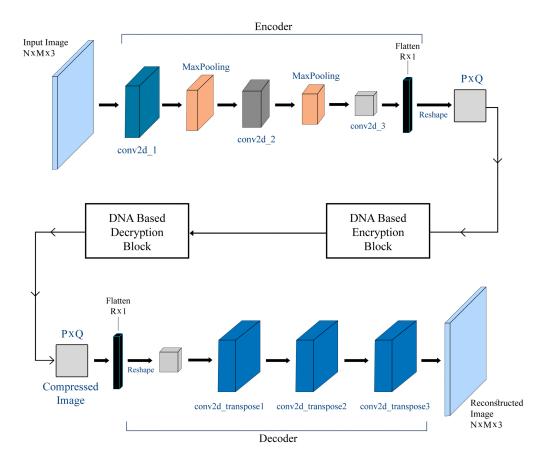
_____
[1]https://r0k.us/graphics/kodak/

Fig. 4. Detailed Architecture of the Proposed Autoencoder along with DNA-based Encryption and Decryption Modules.

4.1 The Proposed Convolutional Autoencoder for Dimensionality Reduction

Autoencoders are artificial neural networks that can be used for image compression using unsupervised learning. If properly trained, they can be used to compress unseen images with an impressive compression ratio. Autoencoders are widely used for dimensionality reduction in generative models of data and contain three components; the encoder, latent vector and decoder. In the encoder, the size of the input is reduced by decreasing its dimension. The middle layer known as a latent vector has a few neurons as compared to the input and output layers. This layer holds the input information but in reduced dimensions named as the latent vector or shortcode. The output is reconstructed through the decoder using the reduced representation from the encoder output. Convolutional Autoencoders (CAE) effectively learn features of the input image in an unsupervised manner by employing a convolutional neural network (CNN). Convolution autoencoders can reconstruct the input image with minimum error. Once the autoencoder model is trained, it can generate a compressed representation of an unseen input image.

Autoencoder Architecture

The proposed autoencoder architecture along with the encryption and decryption modules is shown in Fig. 4. The first part is the encoder in which an input RGB image of size $N \times M \times 3$ (512×786×3) is given as input to the encoder and a gray-scale image having dimensions $P \times Q$ (384×512) is obtained at the output of the encoder. This compressed two-dimensional image can then be used by the encryption module instead of using the original colour image. This greatly helps to improve encryption and decryption speed as it is done in a lower dimension space. The encrypted image is obtained by employing four key-dependent different chaotic maps to randomize the process of permutation and diffusion. The same key is used at the decryption end to successfully recover the gray-scale image. The decrypted image is then given to the decoder module of the autoencoder model. If decryption is correctly done, the reconstructed image from the decoder is perceptually similar to the original colour image with the same dimension. Table 2 shows the architectural details of the proposed autoencoder model. The experimental setup for implementing the autoencoder consisted of Google Colab with 12 GB NVIDIA Tesla K80 GPU and 12 GB ram. Moreover, Keras-based Application Programming Interface (API); v2.10 is used with TensorFlow v2.7 to create deep learning architecture, and OpenCv2-v4.5.5 is used for image dimension correction and normalization in this paper.

Table 2. Convolution Autoencoder Architecture Details.

Neural Network Layer		The Feature Maps	Size	Kernel	Stride	Activation Functions
Input Layer	Input Image	-	512×768×3	-	-	-
1	Conv2d_1	128	512×768×128	3x3	1	ReLU
2	Max Pooling 2D	128	256×384×256	2x2x2	1	-
3	Conv2d_2	64	256×384×64	3x3	1	ReLU
4	Max Pooling 2D	64	128×192×128	2x2x2	1	-
5	Conv2d_3	32	64×96×32	3x3	2	ReLU
6	Flatten	-	196608×1	-	-	-
7	Encoder-Out	-	384×512	-	-	-
8	Decoder-In	-	384×512	-	-	-
9	Flatten	-	196608×1	-	-	-
10	Reshape	-	64×96×32	3x3	-	-
11	Conv2d_transpose1	32	128×192×32	3x3	2	ReLU
12	Conv2d_transpose2	64	256×384×64	3x3	2	ReLU
13	Conv2d_transpose3	3	512×768×3	3x3	2	Sigmoid
Output	Image	-	512×768×3	-	-	-

Coloured input images of size 512×786×3 are fed to the auto-encoder model. Convolution filters of sizes 128, 64, and 32 are used for the encoder part to extract spatial information. The dimension of the input layer is reduced by using Max Pooling. Except for the last layer of the encoder part, all other convolutional layer strides are of size 1. Padding of the same size is used for all the layers. The output after conv2d_3 is $64 \times 92 \times 32$ which contains 32 feature maps but to get a latent vector, this layer has been flattened to produce a vector of $R \times 1$ dimension. For the specific colour image size considered in this paper, R is a latent vector of size 196608. This vector is then reshaped to obtain a 2-dimensional gray-scale image $P \times Q$ (384×512). The compression ratio for this work is 6:1. The gray-scale image is encrypted using the proposed encryption algorithm. Once the gray-scale image is decrypted, it is then given to the decoder part of the autoencoder which uses transpose convolutional filters to regenerate the original input colour image with negligible

loss of information. The proposed CAE model is very lightweight. In terms of trainable parameters, the encoder has 95,840 and the decoder has 29,475 parameters. Due to low training parameters, the compression time is very low for the proposed convolutional autoencoder technique.

Autoencoder Training

The proposed convolutional autoencoder-based deep learning model was trained for different epochs, hyper-parameters and optimizers using the Kodak dataset which has 24 uncompressed similar dimension images. The dataset was divided into a 60% training set and a 40% validation set. The model converged near 550 epochs at the maximum training accuracy of 97% and a loss of 0.0011, whereas the validation accuracy and loss were 95% and 0.0014, respectively as shown in Fig. 5. To avoid overfitting, kernel and bias regularization techniques have been used in all convolution layers for the autoencoder model. L2 regularization with a specific value of $1e^{-6}$ is used to reduce the size of weights, as well as the biases during model training. This helps to avoid overfitting and also removes the fluctuations in model performance metrics. L2 regularization forces small weights to be removed that are very close to zero. This technique improves the model performance.
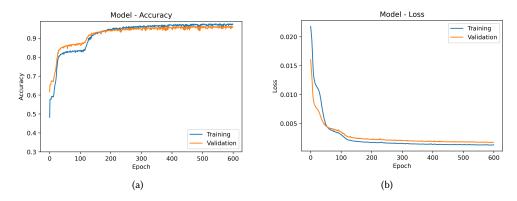

Fig. 5. Model Training Parameters. (a) Autoencoder Training Accuracy Graph. (b) Autoencoder Training Loss Graph

Autoencoder Tuning

Three types of optimizers were tested during the training of the proposed autoencoder model with different hyper-parameter values. The Adam optimizer with an adaptive learning rate was initially selected, but it took very long to improve the training accuracy, therefore, a learning rate of $1e^{-3}$ was used which improved the training speed, but the model accuracy did not improve beyond 88%. The RMSprop optimizer was then used as a replacement for the Adam optimizer with a learning rate of $1e^{-4}$. The model accuracy improved to 90% but still as compared to other research, this accuracy was not enough. The Adamax optimizer with mean-squared-error loss function, $1e^{-4}$ learning rate and 600 epochs, achieved 95% validation accuracy. Data related to model training is presented in Table 3.

Autoencoder Performance

Many researchers have designed deep convolutional neural network-based image compression techniques using different datasets such ImageNet's large database or Kodak's small dataset and various input image sizes. The authors in [11]

Table 3. Experimenting Hyper-parameters and Optimizers.

Hyper-Parameters			
Optimizer	Learning Rate	Epochs	Validation Accuracy
Adam	0.001	500	88%
RMSprop	0.0001	300	90%
Adamax	0.0001	600	95%

claim that their compression technique is close to JPEG2000 but this technique is used for small grayscale images of size 128×128. If the input image size is greater than 128×128, then the large size image will split into non-overlapping small images and each of these samples will be compressed separately. The technique proposed in [11] has produced better results than [6] using the same database but the model was tested on the Kodak database yielding 13.7% BD-rate saving average on all 24 images. The PSNR of the reconstructed images for the same Kodak database is between 29-33 dB.

Quality of the Reconstruct Images using the Proposed Autoencoder Module
Using the proposed autoencoder, a few sample images are shown from the Kodak dataset. Table 4 shows the PSNR values of each image. Specifically, the PSNR value of the Building image is 26 dB, whereas the Field and Shoe images illustrated in Fig. 7 Fig. 8 have PSNR values of 30 and 31 dB, respectively.
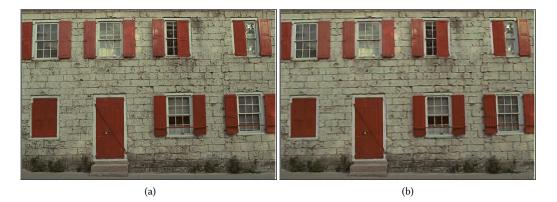

(a)   (b)

Fig. 6. Building Image. (a) Original Building Image. (b) Reconstructed Building Image.

Table 4. PSNR Table for Sample Images.

Images	PSNR(dB)
Building Image	26
Field Image	30
Shoes Image	31

(a)   (b)

Fig. 7. Field Image. (a) Original Field Image. (b) Reconstructed Field Image

(a)   (b)

Fig. 8. Shoe Image. (a) Original Shoe Image. (b) Reconstructed Shoe Image.

4.2   The Proposed DNA based Colour Image Encryption Scheme

Several image encryption schemes employing chaos theory can be found in the literature. Due to sensitivity to initial conditions, chaotic maps produce a secure ciphertext image. But many of these schemes have been cracked and cryptanalysis of such schemes is reported in the literature. Therefore, the encryption scheme proposed in this paper combines chaos and DNA for a high level of security. The proposed encryption scheme has been implemented in MATLAB R2020b on an Intel(R) Core(TM) i7 processor with 16GB of ram.

This section presents the workflow of the proposed colour image encryption scheme. The overall process is illustrated in Fig. 9 and various steps are outlined as follows:

(1) The input colour image having a dimension of N×M×3 is first reduced to a smaller dimension, P×Q, thus forming a gray-scale image I using the proposed convolutional autoencoder module.

(2) Hash of the image I is then taken using SHA-256 to obtain a key K that is sensitive to I. Initial conditions are generated using K and the initial values μ_0 for the TD-ERCS chaotic map, X_0 for the Intertwining chaotic map,
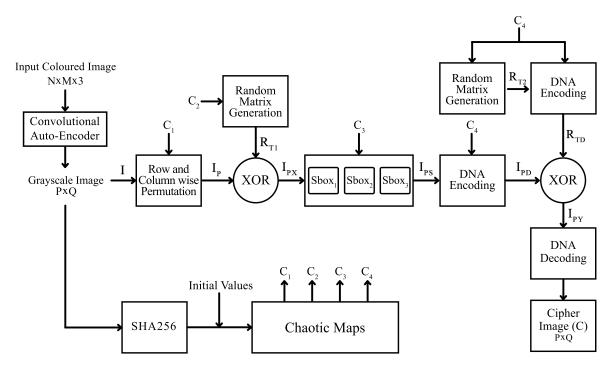
Fig. 9. An All-inclusive Flow of the Proposed Encryption Scheme.

C_0 for the NCA map, and A_0 for the Chirikov chaotic map. The chaotic maps, TD-ERCS, Intertwining, NCA and Chirikov are referred to as C_1, C_2, C_3 and C_4, respectively.

(3) Randomly permutes rows of the image I using the TD-ERCS map C_1 to obtain an intermediate image I_{PR}.

(4) Randomly permute columns of the image I_{PR} using the TD-ERCS map C_1 to obtain the permuted image I_P.

(5) A random matrix is generated using the Interwinning map C_2. Since the values of the random matrix are small, therefore, to scale these values between 0 to 255, multiply each entry of the random matrix by 10^{14} and take modulo 256 to get values in the range 0 to 255. Let this random matrix be referred to as R_{T1}.

(6) XOR I_P and R_{T1} to obtain I_{PX}.

(7) For each pixel of I_{PX}, the NCA map C_3 is used to randomly select one of the three s-boxes. Each pixel value of I_{PX} is then replaced with the corresponding value of the randomly selected S-box. After iterating through all the pixels of I_{PX}, the substituted image I_{PS} is obtained.

(8) Convert the image I_{PS} into a binary matrix and perform DNA encoding by randomly selecting one of the eight DNA rules shown in Table 1. The Chirikov chaotic map C_4 is used for random selection of the rule from Table 1. The DNA encoded image is referred to as I_{PD}.

(9) Generate a random matrix using the Chirikov chaotic map C_4. Since the values of the random matrix are small, therefore, to scale these values between 0 to 255, multiply each entry of the random matrix by 10^{14} and take modulo 256 to get values in the range 0 to 255. Let this random matrix be referred to as R_{T2}.
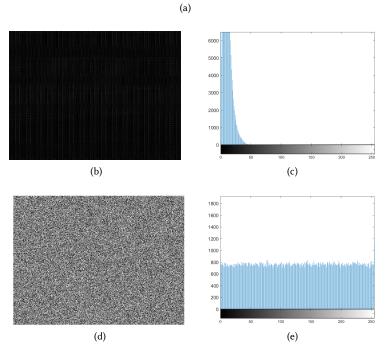
14

Fig. 10. Original Image, Histogram and Cipher Image: The Building Image. (a) Original building image. (b) The Encoded variant. (c) The histogram of the encoded variant. (d) The Encrypted image. (e) The histogram of the encrypted image.

(10) Convert the random matrix R_{T2} into a binary matrix and perform DNA encoding of each entry of R_{T2} by randomly selecting one of the eight DNA rules shown in Table 1. Furthermore, to select a random DNA code from Table 1, the Chirikov chaotic map C_4 is used, which in turn generates the DNA encoded image R_{TD}.

(11) XOR I_{PD} and R_{TD} to obtain I_{PY}.

(12) The cipher image C of dimension $P \times Q$ is obtained by performing DNA decoding of I_{PY}.

5   SECURITY EVALUATION OF THE PROPOSED SCHEME

Several security evaluation parameters, such as histogram of the cipher image, entropy, NPCR, UACI, key sensitivity, contrast, etc., are presented in this section to evaluate the efficacy of the proposed DNA encryption technique.
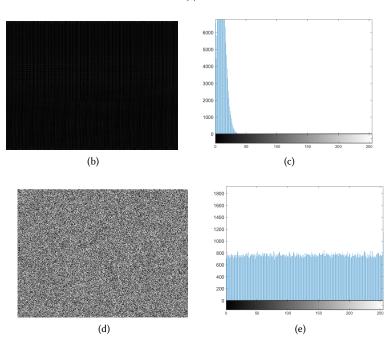
Fig. 11. Original Image, Histogram and Ciphertext Image: Shoe Image. (a) Original Shoe image. (b) The encoded variant. (c) Histogram of the encoded variant. (d) The encrypted image. (e) The histogram of the encrypted image.

5.1 Histogram Analysis

The proposed image encryption scheme was tested on different colour images yielding a flat histogram for the cipher image. For illustration, two different colour images are shown in Fig. 10 and 11. One can see from these figures that the histogram of the encoded images is concentrated more toward the left side and hence it is evident that most of the pixels have values between 0 and 50. Furthermore, the pixel values are randomly distributed in the encrypted images. The histogram of the encrypted image shows that each pixel has approximately the same frequency of occurrence due to which the cipher images have flat histograms.

5.2 Statistical Analysis

It can be observed from the results presented in Fig. 10 and Fig. 11 that the encryption scheme conceals plaintext information. However, only visual inspection cannot guarantee the effectiveness of a good encryption technique. To
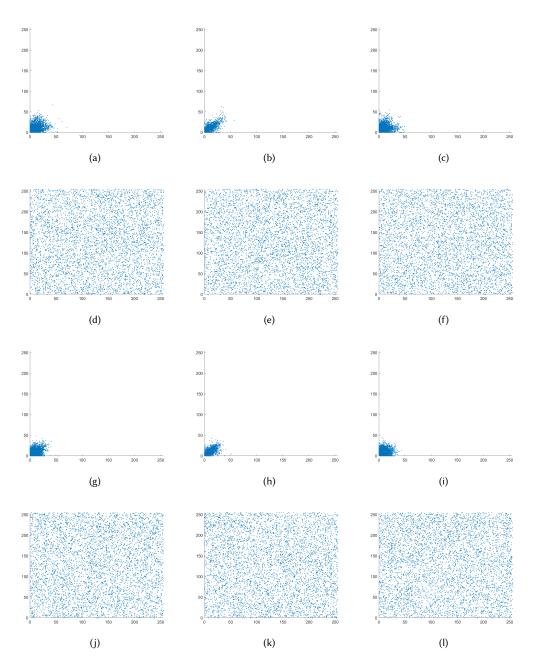
Fig. 12. Correlation Plots of the Original and Cipertext Images; (a-c) Original Image 1, (d-f) Encrypted Image 1, (g-i) Original Image 2, (j-l) Encrypted image 2.

obtain a quantitative assessment, Table 5 exhibits the results after performing different statistical analyses on the two images shown in Fig. 10 and Fig. 11. The values of the encryption parameters [38] obtained in Table 5 demonstrate the

Table 5. Security Analysis of the Encryption Results

Security Metric	Plaintext-Image	Encrypted-Image	Plaintext-Image	Encrypted-Image
Horizontal Correlation Coefficient	0.9612	0.0021	0.9751	0.0026
Vertical Correlation Coefficient	0.9833	-0.0043	0.9712	0.0035
Diagonal Correlation Coefficient	0.9798	0.0033	0.9712	0.0027
E (Entropy)	7.34	7.99	7.39	7.99
KS (Key Sensitivity)	NA	99.33%	NA	99.89%
NPCR	NA	99.78 %	NA	99.85%
UACI	NA	34.25	NA	35.11
C (Contrast)	1.21	10.48	1.24	10.45
H (Homogeneity)	0.71	0.37	0.72	0.36
E (Energy)	0.11	0.02	0.12	0.03

effectiveness of the presented DNA encryption technique. Detail explanation of the encryption evaluation parameters is given below:

Correlation Coefficient: Correlation is a statistical technique for assessing the significance of the correlation between two variables. Correlation is a measure of how closely two variables are linked together. Any cryptosystem's correlation coefficient can be used to assess its level of encryption quality. An image cryptosystem will be considered strong if the encrypted image it produces is random and substantially uncorrelated, and the attributes of the input plaintext image are not present in the cipher image. The correlation coefficient between an encrypted image and the corresponding plaintext image must be exceptionally low if not zero. This means that if two images have a correlation coefficient equal to one, they would be considered identical. Correlation plots for the original and cipher images in different directions are shown in Fig. 12. It is evident from Fig. 12 and Table 5 that the correlation values are close to zero in all the directions. This implies that the pixels of the ciphertext images are uncorrelated. In contrast to the ciphertext correlation values, the original images correlation values are close to 1.

Entropy: The entropy of a source provides insight into self-information or information that a random process provides about itself. Entropy is a critical parameter to study when assessing an encryption method [40]. Assume that we have a truly random source, $m = m_1, m_2...m_8$, which creates 2^8 symbols having the same probability. The entropy value in this ideal scenario will be 8 bits. The entropy values calculated for the input and encrypted images are shown

in Table 5. It is clear from Table 5 that the entropy values of the ciphertext images are close to the ideal desired values.

Key Sensitivity: The key sensitivity test measures how sensitive an encrypted image is to a change in the key. A reliable cryptosystem should decrypt the ciphertext image incorrectly if the key differs by only one bit. For extremely secure cryptosystems, large key sensitivity is necessary and changes in keys should generate a different ciphertext. This is done by calculating the difference between two ciphertext images when the encryption key for the two images is different by only one bit. Table 5 shows the pixel difference between the plaintext and cipher images due to key sensitivity. It is evident from the results shown in Table 5 that the proposed scheme has high key sensitivity, and therefore is sensitive to changes in the secret key.

NPCR and UACI: The impact of a single-pixel change on the total image can be assessed using two standard methods: (i) NPCR and (ii) UACI. Generally speaking, the values of NPCR and UACI should be higher than 99% and 33, respectively. It is evident from Table 5 that the proposed encryption technique achieves adequately high values of the NPCR and UACI parameters.

Contrast: Contrast analysis is a technique that analyzes an image's local intensity variation. An image's texture may be easily identified by a viewer using this statistical metric, which indicates texture uniformity. Varying gray levels can be seen in an image with higher contrast metrics, while images with lower contrast metrics show a lack of variation in gray levels. The contrast results shown in Table 5 demonstrate the fact that the contrast values of the encrypted images are sufficiently higher than the original images.

Homogeneity and Energy: Homogeneity analysis is used to determine the closeness in the distribution of elements in the gray level co-occurrence matrix (GLCM). A low GLCM value of the encrypted image indicates a higher level of security. The energy parameter can be obtained by adding the squared values of the GLCM entries. A low energy value is obtained when the GLCM entries are similar, whereas a high energy value is obtained when the magnitude of some of the entries is greater than others. Secure images require low energy levels. From Table 5, it can be seen that both parameters have lower values thus depicting the effectiveness of the proposed image encryption scheme.

5.3 Comparison of the Keyspace

The total possible combinations of keys that can be utilized in a cryptosystem's encryption and decryption are known as its keyspace size. The number of keyspace available can be used to estimate an encryption algorithm's strength. It has been observed that a minimum keyspace of 2^{100} is required to prevent a brute force attack. The computational precision, according to the IEEE standards, is roughly 10^{15}, due to which there are 10^{285} keys for the proposed encryption technique, and these are significantly higher than 2^{100}. Additionally, the approximate keyspace shown in Table 6 is higher than state-of-the-art encryption schemes.

Table 6. Keyspace analysis.

	Ref [45]	Ref [42]	Ref [29]	Ref [16]	Proposed
Keyspace	10^{75}	10^{96}	10^{170}	10^{168}	10^{285}

6 CONCLUSION

To address the latency issue of encryption/decryption processes for large-size coloured images, a novel deep learning-based encryption scheme using DNA, chaos and multiple s-boxes is presented and evaluated in this paper. The proposed scheme consists of two modules; 1) a deep learning-based convolutional autoencoder to compress the large size three-dimensional coloured images into a significantly lower size two-dimensional gray-scale image, and 2) a novel DNA-based image encryption and decryption module using multiple chaotic sequences and substitution boxes to make the cipher image random as evident from the results reported in the paper. The convolutional autoencoder was trained on the Kodak image dataset with an impressive training and validation accuracy of 97% and 95%, respectively. The results of the autoencoder module demonstrated a high-quality reconstruction of the compressed images into the original colour images with an average PSNR of 29dB. Furthermore, in the proposed image encryption and decryption modules, four different chaotic maps; the TD-ERCS map, the Intertwining map, the Chirikov map, and the NCA map were utilized in conjunction with DNA coding and multiple s-boxes to effectively encrypt digital images. The security of the proposed encryption algorithm was evaluated using several parameters, such as histogram of the cipher image, entropy, NPCR, UACI, key sensitivity, contrast, etc. The results obtained after extensive experimentation revealed the effectiveness of the proposed convolutional autoencoder-based image encryption scheme in terms of; a) the successful compression of large-sized coloured images into low dimension grayscale images, b) the effective encryption/decryption of the compressed images and c) the high-quality reconstruction of compressed images into original three-dimensional colour images. The proposed scheme can effectively be utilized for secure and fast transmission of large-size coloured images over a low bandwidth transmission channel. A symmetric key technique is proposed in this paper for encrypting digital images. Symmetric encryption requires the same key for encryption and decryption. In future, we plan to transform the proposed scheme into an asymmetric image encryption scheme. Another interesting future direction could be to modify this scheme to work for video encryption.

REFERENCES

[1] Nabil Abdoun, Safwan El Assad, Thang Manh Hoang, Olivier Déforges, Rima Assaf, and Mohamad Khalil. 2020. Designing two secure keyed hash functions based on sponge construction and the chaotic neural network. *Entropy* 22, 9 (2020), 1012.

[2] Mohammed Abu Taha, Wassim Hamidouche, Naty Sidaty, Marko Viitanen, Jarno Vanne, Safwan El Assad, and Olivier Déforges. 2020. Privacy protection in real time HEVC standard using chaotic system. *Cryptography* 4, 2 (2020), 18.

[3] Jawad Ahmad and Seong Oun Hwang. 2016. A secure image encryption scheme based on chaotic maps and affine transformation. *Multimedia Tools and Applications* 75, 21 (2016), 13951–13976.

[4] Jawad Ahmad, Hadi Larijani, Rohinton Emmanuel, Mike Mannion, et al. 2018. Secure occupancy monitoring system for iot using lightweight intertwining logistic map. In *2018 10th Computer Science and Electronic Engineering (CEEC)*. IEEE, 208–213.

[5] Prema T Akkasaligar and Sumangala Biradar. 2020. Selective medical image encryption using DNA cryptography. *Information Security Journal: A Global Perspective* 29, 2 (2020), 91–101.

[6] Johannes Ballé, Valero Laparra, and Eero P Simoncelli. 2016. End-to-end optimized image compression. *arXiv preprint arXiv:1611.01704* (2016).

[7] Dalia Battikh, Safwan El Assad, Thang Manh Hoang, Bassem Bakhache, Olivier Deforges, and Mohamad Khalil. 2019. Comparative Study of Three Steganographic Methods Using a Chaotic System and Their Universal Steganalysis Based on Three Feature Vectors. *Entropy* 21, 8 (2019), 748.

[8] Akram Belazi, Muhammad Talha, Sofiane Kharbech, and Wei Xiang. 2019. Novel medical image encryption scheme based on chaos and DNA encoding. *IEEE access* 7 (2019), 36667–36681.

[9] Xiuli Chai, Yiran Chen, and Lucie Broyde. 2017. A novel chaos-based image encryption algorithm using DNA sequence operations. *Optics and Lasers in engineering* 88 (2017), 197–213.

[10] Xiuli Chai, Zhihua Gan, Kang Yang, Yiran Chen, and Xianxing Liu. 2017. An image encryption algorithm based on the memristive hyperchaotic system, cellular automata and DNA sequence operations. *Signal Processing: Image Communication* 52 (2017), 6–19.

[11] Zhengxue Cheng, Heming Sun, Masaru Takeuchi, and Jiro Katto. 2018. Deep convolutional autoencoder-based lossy image compression. In *2018 Picture Coding Symposium (PCS)*. IEEE, 253–257.

[12] Siyamol Chirakkarottu and Sheena Mathew. 2020. A novel encryption method for medical images using 2D Zaslavski map and DNA cryptography. *SN Applied Sciences* 2, 1 (2020), 1–10.

[13] Catherine Taylor Clelland, Viviana Risca, and Carter Bancroft. 1999. Hiding messages in DNA microdots. *Nature* 399, 6736 (1999), 533–534.

[14] Miroslav M Dimitrov. 2020. On the design of chaos-based S-boxes. *IEEE Access* 8 (2020), 117173–117181.

[15] Asha Durafe and Vinod Patidar. 2022. Comparative Analysis of Chaotic Image Encryption Using Improved 2D Gingerbreadman Map and Chirikov Standard Map. In *2022 International Conference for Advancement in Technology (ICONAT)*. IEEE, 1–6.

[16] Marwa Tarek Elkandoz and Wassim Alexan. 2022. Image encryption based on a combination of multiple chaotic maps. *Multimedia Tools and Applications* (2022), 1–22.

[17] Rasul Enayatifar, Abdul Hanan Abdullah, and Ismail Fauzi Isnin. 2014. Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence. *Optics and Lasers in Engineering* 56 (2014), 83–93.

[18] Disha Garg, Komal Kumar Bhatia, and Sonali Gupta. 2022. A novel Genetic Algorithm based Encryption Technique for Securing Data on Fog Network Using DNA Cryptography. In *2022 2nd International Conference on Innovative Practices in Technology and Management (ICIPTM)*, Vol. 2. IEEE, 362–368.

[19] Chirag Gupta. 2020. Shallow Encoder Deep Decoder (SEDD) Networks for Image Encryption and Decryption. *arXiv preprint arXiv:2001.03017* (2020).

[20] Thang Manh Hoang and Safwan El Assad. 2020. Novel models of image permutation and diffusion based on perturbed digital chaos. *Entropy* 22, 5 (2020), 548.

[21] Fei Hu, Changjiu Pu, Haowei Gao, Mengzi Tang, and Li Li. 2016. An image compression and encryption scheme based on deep learning. *arXiv preprint arXiv:1608.05001* (2016).

[22] Fei Hu, Jingyuan Wang, Xiaofei Xu, Changjiu Pu, and Tao Peng. 2017. Batch image encryption using generated deep features based on stacked autoencoder network. *Mathematical Problems in Engineering* 2017 (2017).

[23] Adélaïde Nicole Kengnou Telem, Hilaire Bertrand Fotsin, and Jacques Kengne. 2021. Image encryption algorithm based on dynamic DNA coding operations and 3D chaotic systems. *Multimedia Tools and Applications* 80, 12 (2021), 19011–19041.

[24] Randhir Kumar, Rakesh Tripathi, Ningrinla Marchang, Gautam Srivastava, Thippa Reddy Gadekallu, and Neal N Xiong. 2021. A secured distributed detection system based on IPFS and blockchain for industrial image and video data security. *J. Parallel and Distrib. Comput.* 152 (2021), 128–143.

[25] Qiang Lai, Cong Lai, Hui Zhang, and Chunbiao Li. 2022. Hidden coexisting hyperchaos of new memristive neuron model and its application in image encryption. *Chaos, Solitons & Fractals* 158 (2022), 112017.

[26] Shahid Latif, Maha Driss, Wadii Boulila, Zil E Huma, Sajjad Shaukat Jamal, Zeba Idrees, and Jawad Ahmad. 2021. Deep learning for the industrial internet of things (iiot): A comprehensive survey of techniques, implementation frameworks, potential applications, and future directions. *Sensors* 21, 22 (2021), 7518.

[27] Qi-nan Liao. 2011. TD-RECS Chaotic System Based Digital Image Encryption Algorithm Protecting from Shearing Attack. In *2011 International Conference on Network Computing and Information Security*, Vol. 1. IEEE, 402–405.

[28] Lili Liu, Qiang Zhang, and Xiaopeng Wei. 2012. A RGB image encryption algorithm based on DNA encoding and chaos map. *Computers & Electrical Engineering* 38, 5 (2012), 1240–1248.

[29] C Manikandan, A Gamana, A Sridevi, and Rengarajan Amirtharajan. 2022. Design of tri-layer image encryption scheme using Calendar Month Vowel Count (CMVC) approach. *Multimedia Tools and Applications* (2022), 1–35.

[30] Fawad Masood, Wadii Boulila, Abdullah Alsaeedi, Jan Sher Khan, Jawad Ahmad, Muazzam A Khan, and Sadaqat Ur Rehman. 2022. A novel image encryption scheme based on Arnold cat map, Newton-Leipnik system and Logistic Gaussian map. *Multimedia Tools and Applications* (2022), 1–29.

[31] Fawad Masood, Junaid Masood, Lejun Zhang, Sajjad Shaukat Jamal, Wadii Boulila, Sadaqat Ur Rehman, Fadia Ali Khan, and Jawad Ahmad. 2021. A new color image encryption technique using DNA computing and Chaos-based substitution box. *Soft Computing* (2021), 1–17.

[32] Pratyusa Mukherjee, Hitendra Garg, Chittaranjan Pradhan, Soumik Ghosh, Subrata Chowdhury, and Gautam Srivastava. 2022. Best Fit DNA-Based Cryptographic Keys: The Genetic Algorithm Approach. *Sensors* 22, 19 (2022), 7332.

[33] Suyel Namasudra. 2020. Fast and secure data accessing by using DNA computing for the cloud environment. *IEEE Transactions on Services Computing* (2020).

[34] Suyel Namasudra, Rupak Chakraborty, Abhishek Majumder, and Nageswara Rao Moparthi. 2020. Securing multimedia by using DNA-based encryption in the cloud computing environment. *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)* 16, 3s (2020), 1–19.

[35] Suyel Namasudra, Debashree Devi, Seifedine Kadry, Revathi Sundarasekar, and A Shanthini. 2020. Towards DNA based data security in the cloud computing environment. *Computer Communications* 151 (2020), 539–547.

[36] Chanil Pak and Lilian Huang. 2017. A new color image encryption using combination of the 1D chaotic map. *Signal Processing* 138 (2017), 129–137.

[37] Pramod Pavithran, Sheena Mathew, Suyel Namasudra, and Gautam Srivastava. 2022. A novel cryptosystem based on DNA cryptography, hyperchaotic systems and a randomly generated Moore machine for cyber physical systems. *Computer Communications* 188 (2022), 1–12.

[38] Abdullah Qayyum, Jawad Ahmad, Wadii Boulila, Saeed Rubaiee, Fawad Masood, Fawad Khan, William J Buchanan, et al. 2020. Chaos-based confusion and diffusion of image pixels using dynamic substitution. *IEEE Access* 8 (2020), 140876–140895.

[39] Arslan Shafique, Jameel Ahmed, Wadii Boulila, Hamzah Ghandorh, Jawad Ahmad, and Mujeeb Ur Rehman. 2020. Detecting the security level of various cryptosystems using machine learning models. *IEEE Access* 9 (2020), 9383–9393.

[40] Claude Elwood Shannon. 1948. A mathematical theory of communication. *The Bell system technical journal* 27, 3 (1948), 379–423.

[41] Manreet Sohal and Sandeep Sharma. 2022. BDNA-A DNA inspired symmetric key cryptographic technique to secure cloud computing. *Journal of King Saud University-Computer and Information Sciences* 34, 1 (2022), 1417–1425.

[42] Chunyang Sun, Erfu Wang, and Bing Zhao. 2021. Image Encryption Scheme with Compressed Sensing Based on a New Six-Dimensional Non-Degenerate Discrete Hyperchaotic System and Plaintext-Related Scrambling. *Entropy* 23, 3 (2021), 291.

[43] Kazuo Tanaka, Akimitsu Okamoto, and Isao Saito. 2005. Public-key system using DNA as a one-way function for key distribution. *Biosystems* 81, 1 (2005), 25–29.

[44] Bin Wang, Yingjie Xie, Shihua Zhou, Changjun Zhou, and Xuedong Zheng. 2017. Reversible data hiding based on DNA computing. *Computational Intelligence and Neuroscience* 2017 (2017).

[45] Tao Wang and Ming-hui Wang. 2020. Hyperchaotic image encryption algorithm based on bit-level permutation and DNA encoding. *Optics & Laser Technology* 132 (2020), 106355.

[46] Xingyuan Wang and Yanpei Li. 2021. Chaotic image encryption algorithm based on hybrid multi-objective particle swarm optimization and DNA sequence. *Optics and Lasers in Engineering* 137 (2021), 106393.

[47] Yanfeng Wang, Qinqin Han, Guangzhao Cui, and Junwei Sun. 2019. Hiding messages based on DNA sequence and recombinant DNA technique. *IEEE Transactions on Nanotechnology* 18 (2019), 299–307.

[48] Xianglian Xue, Qiang Zhang, Xiaopeng Wei, Ling Guo, and Qian Wang. 2010. A digital image encryption algorithm based on DNA sequence and multi-chaotic maps. *Neural Network World* 20, 3 (2010), 285.

[49] Xianglian Xue, Dongsheng Zhou, and Changjun Zhou. 2020. New insights into the existing image encryption algorithms based on DNA coding. *Plos one* 15, 10 (2020), e0241184.

[50] Shijie Zhang and Lingfeng Liu. 2021. A novel image encryption algorithm based on SPWLCM and DNA coding. *Mathematics and Computers in Simulation* 190 (2021), 723–744.

[51] Yong Zhang. 2018. The image encryption algorithm based on chaos and DNA computing. *Multimedia Tools and Applications* 77, 16 (2018), 21589–21615.

[52] Ping Zhen, Geng Zhao, Lequan Min, and Xin Jin. 2016. Chaos-based image encryption scheme combining DNA coding and entropy. *Multimedia Tools and Applications* 75, 11 (2016), 6303–6319.