Library Progress International
Vol.44 No. 3, Jul-Dec 2024: P. 16360-16370

Print version ISSN 0970 1052
Online version ISSN 2320 317X

Original Article

Available online at www.bpasjournals.com

Secure Image Encryption using Optimum Key generation with Deep learning Technique in Cloud Storage Environment

S. Sheela[a,b] N. Subbulakshmi [c]

[a]Research Scholar, Department of Computer Applications, Kalasalingam Academy of Research and Education, Krishnankoil, Tamil Nadu, India
[b]Assistant Professor, Marian College Kuttikanam Autonomous Kerala, India
[c] Associate Professor, Department of Computer Science and Engineering, school of computing, Kalasalingam Academy of Research and Education, Krishnankoil, Tamil Nadu, India
Corresponding authors Email: sheelastju@yahoo.com;

How to cite this article: S. Sheela, N. Subbulakshmi (2024) Secure Image Encryption using Optimum Key generation with Deep learning Technique in Cloud Storage Environment. *Library Progress International,* 44(3), 16360-16370

Abstract
Many industries, including healthcare, the military, finance, and more, need extra protection for the interchange of picture data since images are now sent across open channels that might be attacked. In order to protect the system against differential and brute force assaults, the security aspects are crucial. The transmission of multimedia, including digital pictures, text, audio, and video, relies heavily on encryption to maintain secrecy, integrity, and confidentiality while preventing unwanted access to critical information. Even while chaos-based cryptosystems aren't as widely used as AES, DES, or RSA, they've been a hot topic of study recently and can enhance the security of public key cryptosystems when combined with them. With the rise of deep convolutional neural networks (CNNs) as the go-to machine learning technology for many uses, there have been several efforts to use CNNs to decipher encrypted data. On the other hand, prior research has paid little attention to protecting model parameters and has instead concentrated on protecting data. Additionally, they provide high-level implementations without thoroughly analyzing the trade-offs between speed, security, and accuracy in the ECC implementation of common CNN basic operators like non-linear activation, convolution, along with pooling.The goal of this research is to develop and construct a cryptosystem based on Chaos that can effectively encrypt images and withstand differential assaults. In order to create the first layer of encryption, the system first divides the original picture into smaller pieces and rearranges them. A logistic map is used to generate a one-dimensional sequence, which is then multiplied over the highest pixel value and processed bit by bit as part of the encryption process. We use the outcome to encrypt the picture, and then apply the same procedure to decode it. For efficient key generation during picture encryption, the suggested model uses the ECC approach to produce a Dung Beetle optimization (DBO). For improved security performance, the chaotic map notion is introduced to the robust optimization approach. The results of the investigation demonstrate that the suggested approach provides significantly improved security performance while leaving picture quality unaffected.The histogram, Pearson's correlation analysis, peak signal-to-noise ratio (PSNR), entropy, number of pixels change rate (NPCR), and unified average fluctuation in intensity (UACI) are used to assess the encryption outcomes. Our findings prove that the suggested strategy is safe, dependable, efficient, and adaptable.

Keywords: Secure Image Encryption, Cloud Computing Environment, CNN Model, Dung Beetle Optimization, and ECC

1. Introduction

Digital images are becoming a common data format in almost every industry. The proliferation of smartphones, improvements in internet speed, and advances in digital communication have all contributed to the explosion in the amount of media sent over the internet in recent years. Unauthorized parties are more likely to get access to sensitive information, launch attacks, and pose dangers when transfers occur across unsecured channels. Particularly in fields where communication is crucial, such industrial ventures, medical applications, and the military, it is essential to conceal the content of photographs. As a result, people are starting to pay greater attention to the methods proposed for securely storing and sending digital photos. To ensure that unauthorized users cannot easily decipher or access the real visual features,

picture encryption uses cryptographic techniques to transform the content of an image into an unreadable or encrypted version. A secret key is required for decryption since most models use symmetric key methods to encrypt the picture data. Data concealing, watermarking, & image encryption (IE) systems are just a few of the new ways that digital photographs may be protected from possible dangers. Successful and safe IE attempts to encrypt pictures from plaintext such that the receiver may only recover the original image by decrypting it with the correct key. Chaos theory, DNA coding, the Fourier transform, data encryption standard (DES), and advanced encryption standard (AES) are among the IE techniques proposed in the literature.

Every single day, users send and receive vast amounts of data, the majority of which is visual in nature. It is difficult to ensure the confidentiality of data sent via a network while yet making sure that the proper data reaches its intended recipient. There are a plethora of picture encryption techniques available for strong, real-time encryption. Asymmetric and symmetrical encryption techniques are both part of the set. Because of its speed and minimal computational cost, symmetric encryption is well-suited for massive data collections. In symmetric encryption methods, where each user is required to give their secret key before communicating, key distribution and administration create a significant burden. Because asymmetric encryption uses two separate keys for both encryption and decryption, this problem is eliminated. A common asymmetric encryption method, Elliptic Curve Cryptography (ECC) offers better security with lower key sizes and less resource usage, making it a great fit for devices with limited resources. In addition to being simple to develop, fast, and secure against attackers, the model benefits from the unpredictability that chaotic maps provide to encryption methods. Among the many famous chaotic structures used in encryption techniques are the logistic map, the Henon map, the Baker's map, the Arnold Cat map, the sine map, and the Lorenz system. Compared to basic symmetric and asymmetric image encryption techniques that do not use chaos, chaos-based systems are more effective. Improved performance compared to encryption techniques using a single chaotic map was seen when using a mixture of chaotic maps. An established method for improving encryption security and quality involves using higher-dimensional chaotic maps.

Unfortunately, current chaotic maps don't use optimal keys but rather casual key generation methodologies, which results in poor performance and limited chaotic ranges.

1.1 CNN for Image Encryption

Picture encryption is the process of making a picture unintelligible to anybody without the decryption key. This is a crucial loop for acquiring sensitive images and preventing unauthorized access to them. Object identification and picture categorization are two examples of image processing jobs that often use Convolutional Neural Networks (CNNs). Nevertheless, new research has shown that CNNs can also encrypt photos. In convolutional neural network (CNN) based picture encryption methods, the input image's pixel values are garbled. After passing the output of the convolutional layers via a nonlinear initiation capability, the encryption cycle's complexity is further increased. In particular, CNNs' ability to be trained on massive picture datasets to generate very safe encryption algorithms is a major plus when it comes to picture encryption. Also, CNN-based encryption algorithms are fast and effective, so they may be used in real-time.

1.2 Asymmetric Cryptography

One of the most popular forms of encryption is asymmetric cryptography, which is often called public-key cryptography. Unlike symmetric cryptography, which utilizes the same key for both encryption and decryption, public key cryptography employs a public key for encryption with a private key for decryption.

Asymmetric cryptography makes use of ECC, a cryptographic technique based on elliptic curve theory. One possible substitute for the widely used Rivest-Shamir-Adleman (RSA) cryptographic technique for digital signatures is this one. When it comes to creating cryptographic keys, ECC has a number of benefits, including being smaller, quicker, and more efficient. Particularly in settings where computing resources are few, the ECC's efficiency makes it an excellent choice. While using their resources to help extract useful insights from potentially non-shareable material, machine learning on encrypted information can solve privacy and legality problems associated to sharing sensitive data through untrustworthy service providers.

1.3 Identified issues

Data privacy and security are paramount with the growing popularity of storing and processing photos on the cloud, which calls for strong encryption methods. There are gaps in our understanding and vulnerabilities that might be exploited due to the limits of existing picture encryption solutions for cloud settings. This study delves into these issues and suggests ways to improve cloud image security. Through a review of the relevant literature, we have identified significant shortcomings in picture authentication methods, cloud storage security protocols, and algorithmic approaches to image encryption. We then provide ways to secure picture data that use optimization approach based key generating,

ECC encryption, and parallel encryption using CNN. We want to create a more secure and privacy-focused cloud ecosystem for image processing and storage by implementing a system that emphasizes data confidentiality, integrity, and user control.

Robust encryption approaches are required to guarantee the privacy and security of data due to the growing use of cloud-based picture processing and storage. Unfortunately, there are limits to the picture encryption algorithms that are now available for use in cloud settings. This leaves us with gaps in our understanding and weaknesses that may be exploited. In order to improve cloud image security, this study investigates these holes and suggests fixes. Our review of the literature reveals serious shortcomings in picture authentication methods, cloud storage security protocols, and algorithmic approaches to encrypting and decrypting images. Afterwards, we provide ways to secure picture data that use ECC encryption, CNN-based parallel encryption, and optimization-based key generation. A more private and secure cloud environment for picture processing and storage may be achieved with our suggested system's emphasis on data secrecy, integrity, and user agency.

This article delves further into the topic of picture security by discussing the several CNN-based encryption algorithms, their pros and cons, and possible uses in the industry. In this part, it evaluates state-of-the-art picture encryption methods alongside CNN-based encryption algorithms.By merging elliptic curve and homomorphic encryption, we provide a new and enhanced approach for encrypting medical images. It improves key space while sensitivity by modifying standard ECC. This approach shows great promise for medical picture security, since experimental findings show enhanced encryption and resistance against exhaustive and statistical assaults.

What follows is an overview of the article's structure. Part II provides a rundown of the necessary prerequisites. Section III includes the specifics of the suggested approach. In Section IV, we detail the simulation, examine the outcomes, and draw comparisons. At last, the paper's conclusion is found in Section V.

2. Related Work

Introduces a new permutation method called orbital-extraction permutation in an image encryption approach that is presented in [11]. Modules for key generation, orbital-extraction permutation, and dynamic chaotic replacement make up the proposed encryption method. The 2D Hénon map, a chaotic and very non-linear map, is used by the key generation component to create cryptographic keys. By complexly rearranging the pixels of the plain text picture, the orbital-extraction permutation module destroys the intrinsic association between nearby pixels in the input image. A robust diffusion stage is provided by the suggested permutation method. Not only that, bit-XOR operations as well as chaotic substitution procedures have been used for the encryption scheme's confusion element. Important statistical security characteristics have been tested using the suggested approach. The results show that the suggested method is more secure and resilient than before, with an information entropy of 7.9974 with a correlation coefficient of 0.007.

An innovative chaotic log-map, deep convolutional neural network (CNN) approach, and bit reversion operation are the building blocks of a trustworthy and secure picture encryption technique described in [12]. To improve the scheme's key sensitivity, CNN is used to create an image-based public key. In order to generate a chaotic sequence for the encryption processes, the key is employed to acquire the initial values and regulate parameters for the chaotic log-map. The system proceeds to encrypt the photos via permuting, DNA encoding, diffusing, and bit reversing, all of which manipulate and scramble the pixels of the images. A number of cryptanalyses, including key-space, key sensitivity, data entropy, histogram, correlation, divergence attack, noisy assault, and cropping attack, are used to thoroughly evaluate the encryption technique for the famous photographs. The picture encryption approach is further supported by comparing the numerical and visual outcomes to existing state-of-the-art scores. Consequently, the suggested method of encrypting images using log maps has been confirmed and validated by top-notch comparative and absolute findings. It is possible to expand the suggested log-map to combinational multi-dimensional using current efficient chaotic maps as an area for future research. To protect the system against differential and brute-force assaults, the elements listed in [13] must be in place. Our proposed Enhanced Logistic Map (ELM) employs chaotic maps and basic encryption methods to protect it from assaults. These methods include block scrambling, altered zigzag transformations for encryption phases (which includes diffusion and permutation), and key stream generation.

As an example of a steganographic application, digital picture steganography was created and used to conceal text in the chosen photos in the research [14]. During this process, the discrete Haar wavelet transformation of the initially acquired pictures will be used to conceal data in the low bands. A one-time pad algorithm is used to encrypt the text that has to be concealed. An algorithm for highly secure information exchange serves as the foundation for the transmission layer that conveys the encryption key to the recipient. Both the sender and the receiver keep a key pool that is produced at random and used by the algorithms. For each message, a new random key start point is generated, and then a key is randomly

picked from the pool. A one-time pad must ensure that no key is repeated, and two crucial elements in this regard are the size of the pool and the randomization. Underneath the images, using the least important bit approach, are the ciphertext and key beginning point indication concealed. The pre-stego photos were subjected to the ideal pixel modification procedure, leading to enhanced outcomes. In this study, we compare our findings to those of previous research as well as to those of the pre-optimal pixel correction technique. Among the metrics measured by the tests, the suggested technique had the best performance with regard to peak signal- to-noise ratio, structural similarity index, mean absolute error, mean consequential error, and encryption key security.

Particle swarm optimizing, chaotic maps, and magic squares are used in the technique to provide an optimal encryption effect in [15]. In this paper, a new magic square-based encryption technique is presented. The picture is first decomposed into 1-byte chunks, and the magic square's value is then substituted for each of them. The PSO optimization procedure then makes use of the encrypted pictures as particles for initial assembly. As a fitness function, the optimal encrypted picture is defined by applying the correlation coefficient to nearby pixels. Experiments show that the suggested method successfully encrypts pictures with different secret keys and produces respectable encryption results. Because of this, the suggested work increases memory economy and strengthens the security of the public key technique.

Ellipstic curve cryptography (ECC) is an intriguing method among the methods mentioned in [16] for keeping picture data safe and private. The ECC method's key generation procedure creates both the private and public key pair that are used for picture encryption and decryption. The public key is created at random while encryption is taking place. An optimization strategy based on genetic algorithms (GAs) is used to produce the private key (H) in the decryption process of the proposed method. The picture quality is assessed by employing the PSNR value as a fitness metric for optimization. Therefore, when compared to other approaches, the suggested one provides the best PSNR value.

3. Proposed Work

3.1 System Model

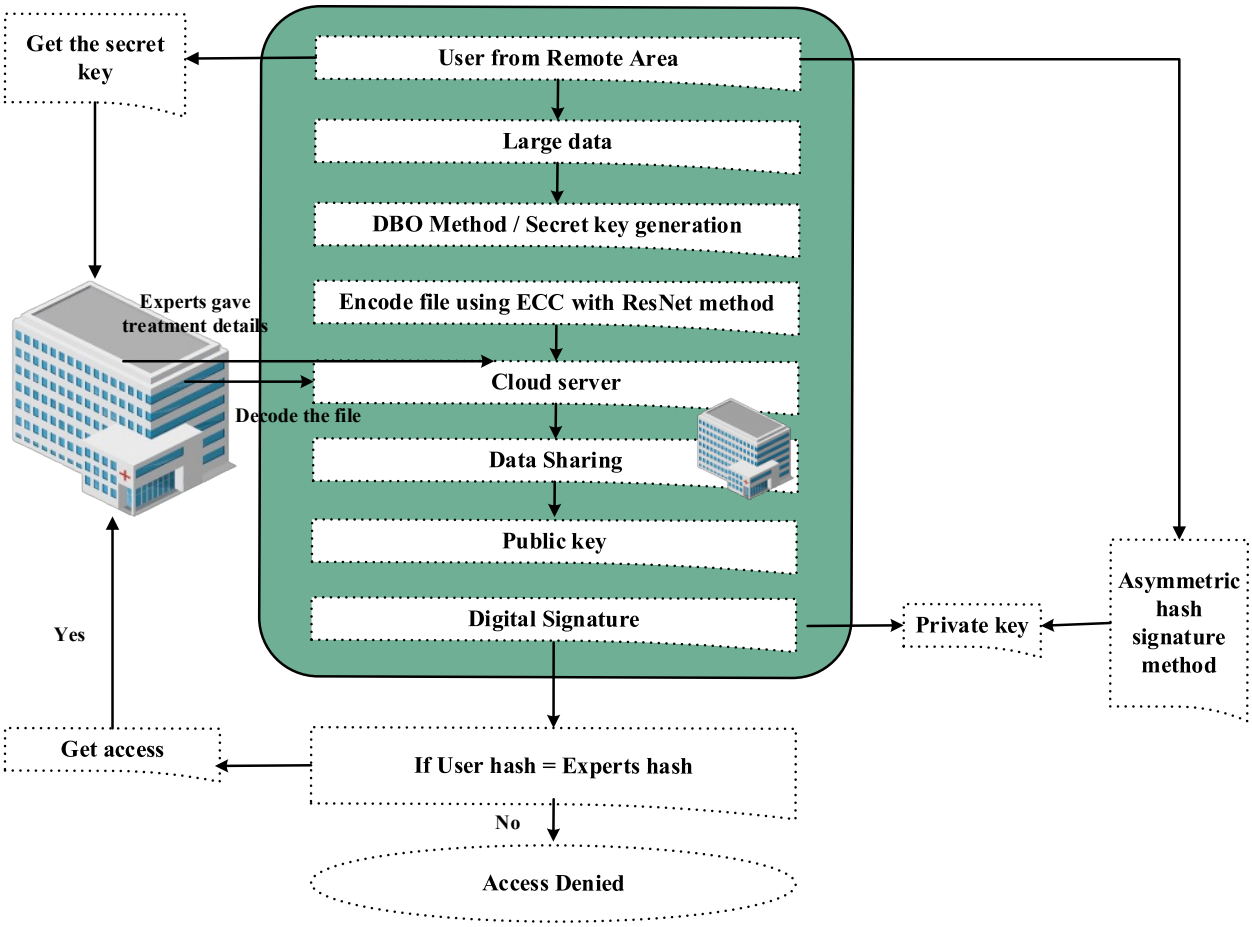

Fig.1. Proposed Model using CNN with ECC

To demonstrate our point, we use a standard Resnet design in this study. Implementing a Resnet on encrypted inputs requires overcoming two major obstacles, even though ECC systems permit arbitrary calculations on the encrypted data.

Improving the efficiency of the Single Instruction Multiple Data (SIMD) processes begins with correctly packing the input data. Next, apart from polynomials, the majority of ECC schemes can't directly calculate non-linear functions, which presents its own set of problems. A polynomial function or iterative approach is often used to approximate the non-linear function. You need to be cautious managing the trade-off among computational depth with accuracy while the approximation error is often inversely related to the former (more iteration or higher-degree polynomial lead to less approximation error).

3.2 Optimization based Key generator

The technique of generating ECC keys using genetic algorithms combines the cryptographic features of elliptic-curve cryptography with the concepts of genetic algorithms to produce key pairs that are both safe and effective. The procedures for the proposed technique are detailed in this section:

The DBO method has great optimization accuracy and fast convergence. Regardless, there is a disparity between the global prospecting capacity and the local searching capacity. Put simply, the DBO algorithm isn't great at exploring the world and is prone to becoming stuck in local optimization traps. In light of this, we resolve the aforementioned problems by using three tactics for improvement.

Dung Beetle Initialization and Representation: A Dung Beetle, in the context of ECC, represents an elliptic-curve point. It all starts with initializing a colony of Dung Beetles. The two pieces that make up a Dung Beetle are the coordinates for x and y. These coordinates are generated at random from the parameter space of the curve. The population size, which is the number of possible key pairs being assessed, is determined by a user-defined parameter.

Health Assessment: A Dung Beetle's (the curve's) closeness to a predetermined target point is assessed by the fitness function. A public key that is desired may be represented by the target point. In order to determine how far away the target point is from the current location of the Dung Beetle, the fitness function uses a formula. Dung beetles are more fit when the distance is less. By simulating their proximity to the target location, Dung Beetles are thought to be more likely to indicate desired key pairings.

The following are the revised procedures for populace initialization:

(1) Find the dimension of the optimization problem, which is the number of prime integers D.

(2) For every prime number, establish a range [Lb,Ub] with Lb being the lower bound and Ub being the upper limit.

(3) For any prime number, there are N equal subintervals in the range [Lb,Ub]. N is the DBO algorithm's population size.

(4) Make sure the matrix has dimensions N×D. The numbers 1, 2... N are sorted randomly in each column. The next step is to randomly choose a subinterval's worth of rows as a sample. The starting population is the end product.

The algorithm's variety, exploration capacity, and convergence speed are greatly affected by the values assigned to these parameters. Interactions between ECC and DBO: Through the fitness function, ECC and DBO interact with one another. The fitness function, the goal point, and the curve parameters are all supplied by ECC. Using the fitness function described by the ECC, the DBO creates prospective key pairs, which are really Dung Beetles, and then determines how well they perform. In order to find key pairings that are in line with the goal point, DBO repeatedly evolves the population, driving the exploration and extraction process. Using evolutionary principles, the DBO-based ECC-key-generation process optimizes the formation of safe key pairs. The technique aims to find points that are similar to the goal point by repeatedly developing populations of Dung Beetles, where each point represents an elliptic curve. The DBO maintains a healthy equilibrium between exploitation and exploration via fitness assessment, ball-rolling dung beetles, brood balls, little dung beetles, and stolen dung beetles in order to make ECC-key-pair production more efficient and secure.

3.3 DL based Image Encryption and Decryption

Here, Convolutional Neural Networks (CNNs) are used to encrypt images. We used the ResNet-18 convolutional neural network that had already been trained. Using over a million photos from the ImageNet database, an 18-layer network was trained. This pre-trained network is capable of classifying pictures into a thousand different item types, including pencil, mouse, keyboard, even a plethora of animal pictures. So, with a big set of photos, the network learned a lot of features. Using pre-trained networks for transfer learning is often more efficient and simpler than training a custom convolutional network from beginning. Figure 3 shows the suggested network model design. In the convolutional layers of the 18-layer network, there are 3 × 3 filters. The network is configured so that, in the event that the output feature map is of an identical size, the number of filters matches the number of layers. Filters are twice in layers when the output feature map is divided in half. The down sampling is carried out using convolutional layers with a stride of 2. Interlayer connections are used to inject the remaining shortcut connections into the networks. You may think about relationships in two categories. Solid lines represent the first kind, which is used where the dimensions of the input and the result are same.

This kind is called the dashed lines, whereas the other type is utilized when the dimensions are increased. Using a stride of 2 for expanded dimensions, this sort of connection has been used for identity mapping, albeit with zeros padding.

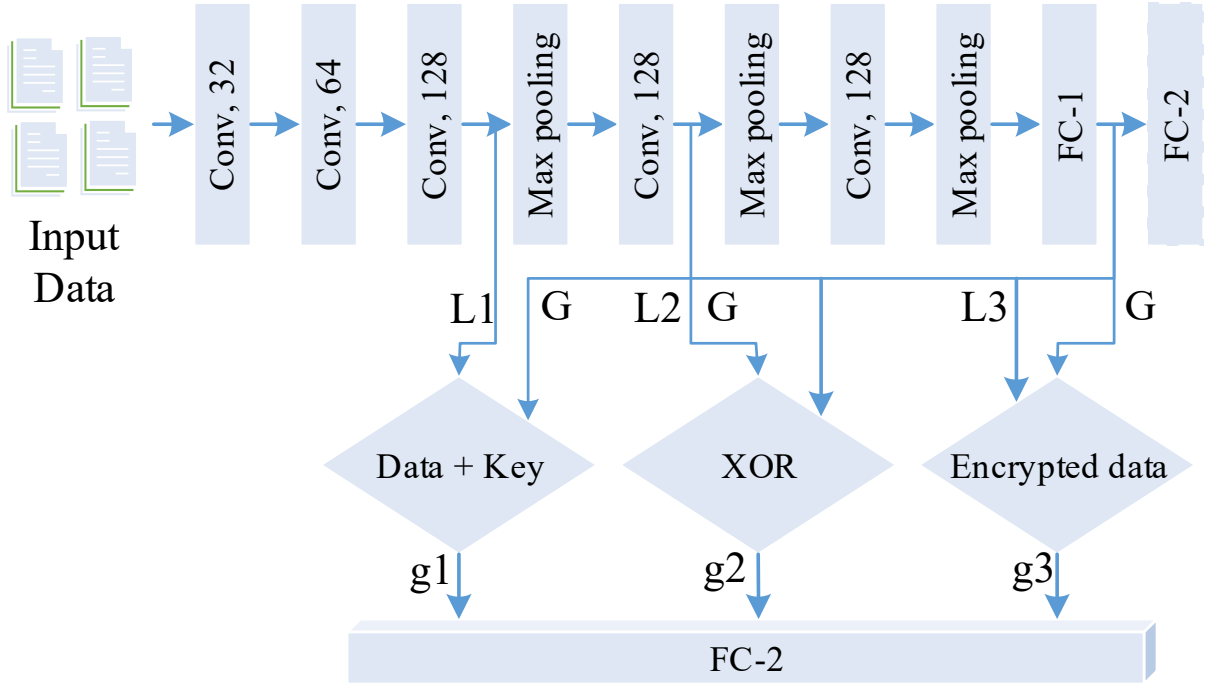

Fig.2. CNN with ECC for Encryption

Video and image data are common inputs for convolutional neural networks (CNNs), which consist of many layers of neural connections. The network's layer l(l=1,2,⋯,D) input and output are represented by X(l) and Z(l), respectively. As an example, X(l)=Z(l-1), where Z(0) is the initial input data, and each network layer applies its own unique mathematical operation on the outputs of the layers below it before passing them on to the next layer. Starting from the raw data, this structure enables the computation of higher-level abstract characteristics as non-linear coefficients of lower-level features. These three kinds of processes typically make up a CNN's first few layers.

Convolution: The procedure is linear, and it produces a filtered output Y by convolving the input to layer ^2 (X) with a kernel (W). The element in the i-th row and j-th columns of a matrix A is denoted as A_(i,j). Imagine that the dimensions of the input X are (M×N) and that the dimensions of the kernel W are (P×Q). To calculate the filter outputs at the edges, it is common practice to pad the input using zeros. X ̧ represents the input X with zero padding removed.

$$Y_{m,n} = \langle \hat{X}_{m,n}, \widehat{W} \rangle$$

where $\langle a, b \rangle$represents the inner product of two vectors a and b, Wˆ stands for the vectorized (flattened) variation of the kernel W, and $\hat{X}_{m,n}$ is the vectorized form of the input window taken from the padded picture. This window has dimensions P×Q and $\hat{X}_{m,n}$ is the top-left element. To keep things simple, we'll suppose that the stride length is 1 in equation (1).

Activation: A non-linear function applied point-wise to the filter responses is used here. Rectified linear unit (ReLU), sigmoid, and hyperbolic tangent (tanh) are three well-liked activation functions. The function of ReLU activation is defined as follows in this study:

$$Re\ LU(a) = max(0, a) = \{0,\ if\ a \leq 0\ a,\ if\ a > 0$$

Pooling: One common use is dimensionality reduction, which involves combining many replies from the same region. A linear process, mean pooling calculates the average response for every neighborhood, in contrast to the non-linear max pooling, which is often used to choose the most dominating response in each neighborhood. A non-linear function f(Y) may be used to simulate the activation as well as pooling layers' final output (Z) as a function of the filter responses.

The data is transformed into a vector while a few fully linked (FC) layers are included into the network after the first ones. Using an activation function that is not linear to the weighted average of the inputs—which always emits value 1—of all the nodes in the FC layer is a common approach to calculate its output. The equation Z=f(WX) may be used to express this, where W is the FC layer's weight matrix and f is an activation function. A softmax layer, which approximates the probability distribution across the class labels, is often the last layer in a CNN.

The training parameters for Resnet models are 512 batches and 20 epochs. The number of rows utilized at once in a batch

is represented by the batch size, and the number of epochs is the total number of times a model is trained using the data set. Two megabits (mbits) is the definition of the message space, where mbits is the 16-bit message length. Dividing the message space with the batch size yields 2500 iterations as the total amount of iterations per epoch.Every message gets its own unique set of keys when the ResNet model is trained. This procedure requires 512 bunches of public/private keys and 512 batches of 16-bit messages. The Eve model follows the identical procedure, with the exception of the private key cannot be accessed.

The network arranges the input photographs in a hierarchical fashion. In subsequent levels, you may find higher-level characteristics that were learned from the lower-level features in the layers above. In order to get feature representations of both the training and test data at the end of the network, activations on the global pooling layer, known as "pool5", are used. By using the global pooling layer to aggregate the input features across all geographic regions, we are able to acquire 512 features in total. We get a number between zero and one using these picture attributes. The last step is to compare these numbers to 0.5 in order to turn them into binary. If these numbers are lower than half, they will be set to zero. Then their number will be 1.

4. Results & Discussion

This model was built on an HP laptop with an Intel(R) Core(TM) i5-8250U CPU@1.80GHz and 8GB of RAM using Python 3.7 and the Spyder 4.1.5 integrated development environment. An encrypted 512-bit curve from ECC Brainpool is used as the elliptic curve in the suggested technique. You may see the implementation-related elliptic curve parameters in Table 1.

In this research, the parameters used for EC in 64-bit are p = 113, a = −1, b = 17, with G = (52, 61). The Lena, Barbara, and Mandrill grayscale pictures are considered. The RGB photographs that were used as inputs are Lena, House, while Mandrill. In order to compare the outcomes, the suggested procedure will be applied to both grayscale and Lena photos. A cipher system's robustness is assessed by looking at how well it fares against several types of assaults, such as known plaintext attack, statistical attack, differential attack, brute force attack, along with ciphertext attack. A safety study was carried out on the suggested method to assess it. This analysis included discussing entropy, histograms, the NIST and randomness tests, MSE, UACI, and the correlation coefficient NPCR.

An indicator known as the Peak Signal to Noise Ratio (PSNR) shows the relationship between the greatest allowable mean squared disagreement between any two pictures and the fraction of the mean squared variance among pixel values in two different images. The PSNR score is usually expected to be lower in a cipher image situation. In contrast, SSIM is a measure that may be used to quantify the level of similarity between two photographs. The SSIM result might be anywhere from -1 to 1, while 1 indicating that the compared pictures are identical. The PSNR and SSIM of the encrypted and decrypted images are compared in Table 2.

The Scaled Score for Image Similarity (SSIM) index takes values between 0 and 1 to indicate how similar two pictures are. Human subjectivity is strongly supported by SSIM. Blocks are created by dividing the whole spatial region using the SSIM method. All the SSIM values add up to a picture's total quality, and each SSIM value represents the level of a single block's pixels. A high mean SSIM indicates a high degree of similarity between the attacked and reconstructed images, since it includes more white pixels in its SSIM map. One way to describe SSIM is as

$$SSIM\ (x,y)\ = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1) + (\sigma_x^2 + \sigma_y^2 + c_2)}\ c_1\ = (K_1L)^2, c_2 = (K_2L)^2$$

where μ_x and $\mu_y$signify the mean of x and y, σ_x and $\sigma_y$signify the variance of x and y, σ_{xy}means the standard deviation of the data, L stands for the pictures' dynamic range (which is 255 by default), and K_1 and K_2 are constants with default values of 0.01 and 0.03, respectively.

In general, unencrypted pictures tend to be homogeneous and show high pixel correlations on all three dimensions. There is a security concern in picture encryption when there are strong correlations among the original with encrypted images, since they might reveal patterns. To improve security by reducing keeping data from the initial picture, the small correlation coefficient is crucial in image encryption. The following equation is used to compute the correlation coefficient:

$$Cc[v1, v2] = \frac{Covariance\ [v1, v2]}{SD[v1] \times SD[v2]}$$

where,

Cc: Correlation coefficient.

SD: Standard Deviation.

Table 1

Achieving encryption using the suggested approach using five photos.

Test Images	MSE	RMSE	PSNR (dB)	CC (%)
IMG_1	0.045	0.212	61.599	99.78
IMG_2	0.076	0.276	59.323	99.92
IMG_3	0.038	0.195	62.333	99.89
IMG_4	0.078	0.279	59.210	99.92
IMG_5	0.103	0.321	58.002	99.98
IMG_6	0.067	0.259	59.870	99.86

Table 4 compares the suggested method's correlational coefficients to those of other comparable approaches that are already in use. The general rule is that a higher PSNR value will result in better reconstruction and less distortion. On occasion, however, PSNR's depiction of picture quality does not correspond to how humans subjectively perceive visual objects. The picture quality in the high frequency region is higher than the other two when white noise is applied to the same image in that order; nonetheless, the PSNR levels of the three areas are identical. For this reason, we also computed the SSIM to provide a more accurate assessment of the picture quality.

One way to measure the efficacy of an image encryption structure is by looking at its diffusion performance. What this means is that the pixels in the plain picture affect the pixels in the cypher image in very noticeable ways. At now, a new cypher picture is required in order to evaluate the resistance to the differentiating assault; this is because the plain image may be changed by one bit and the changes in the cypher images can be compared. Two quantitative measurements, the average intensity of uniform shift and the rate of pixel variation (NPCR) are used to guarantee the image coding method against differential assault.

$$N_{NPCR} = \frac{\sum_{i,j} \quad Di,j}{M \times N} \times 100\% \; UACI = \frac{1}{M \times N} \frac{\sum_{i,j} \quad c_1 i,j - C_2 i,j}{255} \times 100\%$$

in where M is the plain image's width and N is its height, and C_1 (i,j) along with $C_2 i,j$ are the pixel values at position (i,j) in the two cipher images, respectively. The following is the specification of D(i,j): the number of gray levels is 255, C_1 and C_2 are the plain images before and after modifying one bit; and:

$$Di,j = 0, \; for \; C_1 \; i,j = C_2 i,j \; 1, \; for \; C_1 \; i,j \neq C_2 i,j$$

The theoretical values of UACI are 33.46 and NPCR is 99.61%. Gaining NPCR and UAC/ values that are higher than or equal to these anticipated levels results in a more robust and secure coding scheme. According to the proposed method, we adjusted the value of a single randomly selected pixel, computed C_1 and C_2 cipher images representing the original and modified pictures, respectively, and then determined NPCR and UAC/ for each image. Table 7 displays the outcome.

Table 7. NPCR and UACI values for Lena Image

Algorithm	Image Size	Encryption		Authentication
		NPCR %	UACI %	
IMG_1	512 × 512	99.61	33.47	✓
IMG_2	512 × 512	99.61	33.48	×
IMG_3	512 × 512	99.61	33.49	×
IMG_4	512 × 512	99.60	33.46	×
IMG_5	512 × 512	99.61	28.61	×

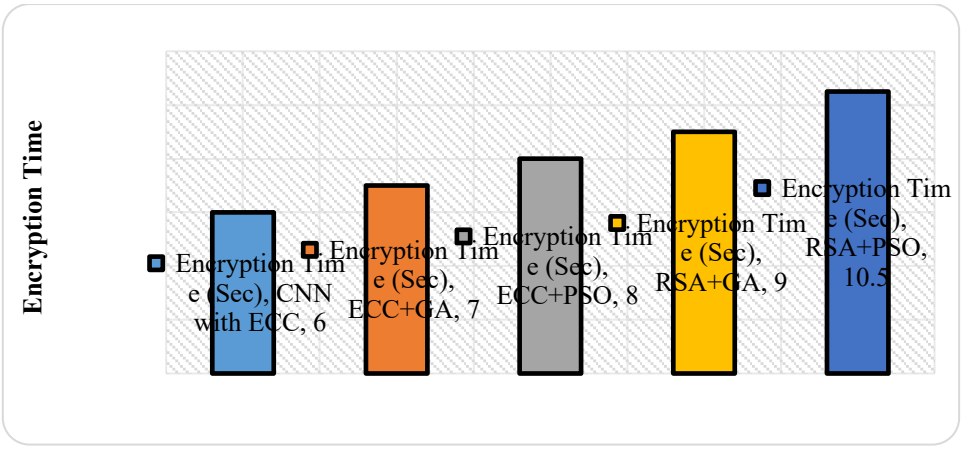

Fig.3. Encryption time

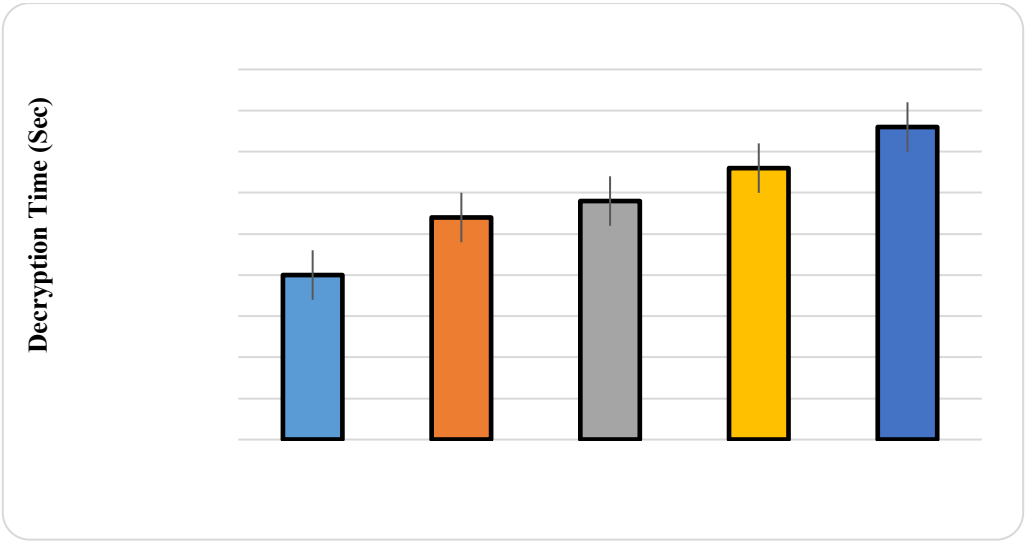

Fig.4. Decryption time

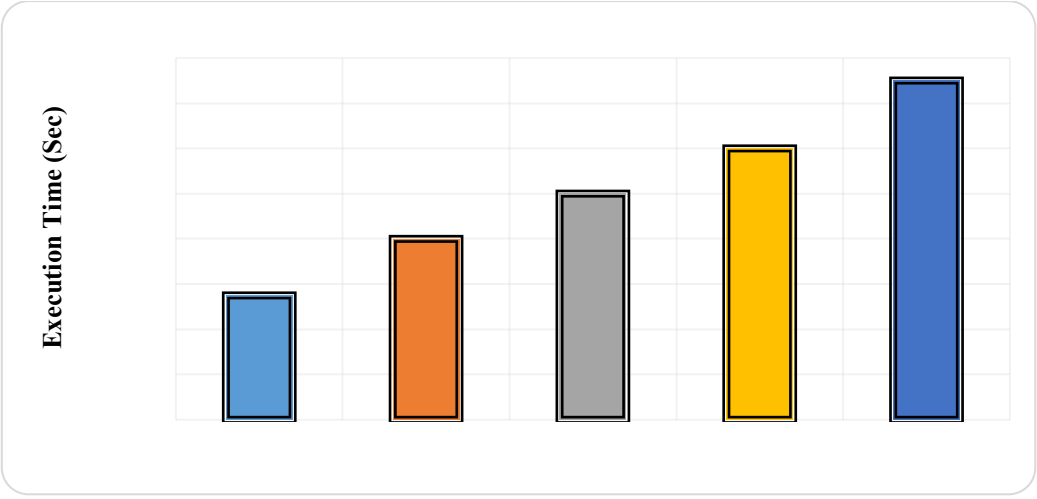

Fig.5. Execution time

After extensive comparison with comparable approaches already in existence, the suggested algorithm proved to be much more efficient in terms of the duration of execution. It has routinely outperformed competing approaches in comprehensive benchmark testing. This advantage becomes much more important in contexts where processing speed is paramount, such as in real-time applications. Time required to encrypt and decrypt using various techniques is shown in Fig. 6.

Security Attacks Analysis

Robustness of ECC-ResNet Approach against Cryptographic Attacks

Protecting sensitive information requires a cryptographic method that is both strong and reliable. Testing the ECC-ResNet method's resistance to prevalent cryptographic attacks and flaws is crucial as it adds a new level to key generation via evolutionary algorithms. We talk about how the ECC-ResNet method may be resilient here:

- **Brute Force Attacks:** In a brute force assault, every conceivable key combination is tried until one works. Because it can efficiently explore a larger solution space, the ECC-RESNET method may increase resilience against such assaults.
- **Randomness Vulnerabilities:** The independence of private keys is crucial for the generation of safe key pairs. By using a genetic algorithm, ECC-RESNET adds a stochastic process that may increase the produced keys' unpredictability.
- **Key Enumeration Attacks:** By taking advantage of trends in key creation, key enumeration attacks narrow the search field. Because of ECC-RESNET's exploration capabilities, counter key enumerated attacks may be more difficult to launch.

Computational Complexity Analysis

We further united it under the Gaussian interference game paradigm in (9), which allowed us to solve the original NP-hard issue in (6). As evidence of the optimization methods, we see the possibility of using DRL approaches on different networks with restricted resources. To further simplify calculation, a DRL-based approach is created that incorporates experience replay. Several training scenarios are used to test the effectiveness of the DQL-based power allocation model. These scenarios include growing cell user demands and varied transmit power budgets. On average, we have put 9–10 trials with random initializations through the learning process. The two distinct DQN functions—the train DQN and the learning target DQN having parameters set—inherently handle the computing complexity of the learning process. To evaluate the effectiveness of various power allocation strategies, we compare their optimization solutions using sum rate performance measures. Compared to existing power allocation approaches, the suggested DQL methodology clearly outperforms them in the numerical simulations.

The scale of the wireless network is the primary determinant, as one would anticipate, of the DRL algorithm's complexity. The average cumulative throughput performance of the suggested DRL-based strategy steadily drops as the total number of destination receivers increases, as shown in Figure 5. Increasing the number of mobile users leads to a larger wireless network and a correspondingly larger state-action space. The learning system is thus able to discover more exploration parameters for estimating the best action-value functions. Consequently, as the number of cell users increases, the sum-rate effectiveness of the DQN system steadily diminishes.

5. Conclusion

The suggested methodology for authenticating and encrypting photos uses discretized ECC to improve the encryption quality of both color and grayscale images in cloud storage. By actively preventing Chosen-Plaintext (CPA) and Known-Plaintext (KPA) attacks, the model improves cipher picture quality in comparison to current schemes that have greater entropy, lower association, higher average NPCR as well as UACI, lower PSNR as well as SSIM values, and so on. Statistical and cryptanalytic assaults were no match for the suggested model's resilience, portability, and competence. In order to accommodate more types of real-time multimedia encryption—audio, video, and more—in future efforts, the encryption model may be modified in cloud storage.

References

1. Prabhu, D., Bhanu, S.V., & Suthir, S. (2023). Modeling of Optimal Multi Key Homomorphic Encryption With Deep Learning Biometric Based Authentication System For Cloud Computing. ASEAN Engineering Journal.
2. Raja, N.K., Lydia, E.L., Acharya, T.A., Radhika, K., Yang, E., & Yi, O. (2023). Rider Optimization With Deep Learning Based Image Encryption for Secure Drone Communication. IEEE Access, 11, 121646-121655.
3. Raja, N.K., Lydia, E.L., Acharya, T.A., Radhika, K., Yang, E., & Yi, O. (2023). Rider Optimization With Deep Learning Based Image Encryption for Secure Drone Communication. IEEE Access, 11, 121646-121655.
4. G, C.A., &Basarkod, P.I. (2022). A Novel Approach of Smart Contract based Distributed Ledger Technology using Deep Learning Techniques to Secure Medical Images. 2022 International Conference on Knowledge Engineering and Communication Systems (ICKES), 1-6.

5. Selvakumar, K., & Lokesh, S. (2024). Deep-KEDI: Deep learning-based zigzag generative adversarial network for encryption and decryption of medical images. Technology and health care : official journal of the European Society for Engineering and Medicine.
6. Lata, K., &Cenkeramaddi, L. (2023). Deep Learning for Medical Image Cryptography: A Comprehensive Review. Applied Sciences.
7. Kalphana, K.R., Aanjankumar, S., Surya, M., Ramadevi, M.S., Ramela, K.R., Anitha, T., Nagaprasad, N., &Krishnaraj, R. (2024). Prediction of android ransomware with deep learning model using hybrid cryptography. Scientific Reports, 14.
8. Sammeta, N., & Parthiban, L. (2021). Hyperledger blockchain enabled secure medical record management with deep learning-based diagnosis model. Complex & Intelligent Systems, 8, 625 - 640.
9. Eshmawi, A.A., Khayyat, M.M., Abdel-Khalek, S., Mansour, R.F., Dwivedi, U.K., Joshi, K.K., & Gupta, D. (2022). Deep learning with metaheuristics based data sensing and encoding scheme for secure cyber physical sensor systems. Cluster Computing, 26, 2245 - 2257.
10. Anitha, M., Arulanantham, D., Brinda, G., Vijayakumar, S., Prakash, G., & Shivaranjani, M. (2023). Enhancing IoT Image Security Through Hybrid Encryption and Optimal Key Generation with Optimization. 2023 International Conference on Self Sustainable Artificial Intelligence Systems (ICSSAS), 1355-1362.
11. Khan, S., Ullah, S., Ahmad, J., Ullah, A., Arshad, A., & Khan, M.S. (2024). Image Encryption Using A Novel Orbital-Extraction Permutation Technique and Chaotic Key Generation. 2024 IEEE 7th International Conference on Advanced Technologies, Signal and Image Processing (ATSIP), 1, 414-419.
12. Erkan, U., Toktas, A., Enginoğlu, S., Karabacak, E., & Thanh, D.N. (2020). An image encryption scheme based on chaotic logarithmic map and key generation using deep CNN. Multimedia Tools and Applications, 81, 7365 - 7391.
13. Ramasamy, P., Ranganathan, V., Kadry, S.N., Damaševičius, R., &Blažauskas, T. (2019). An Image Encryption Scheme Based on Block Scrambling, Modified Zigzag Transformation and Key Generation Using Enhanced Logistic—Tent Map. Entropy, 21.
14. Takaoğlu, M., Özyavas, A., Ajlouni, N.M., &Takaoglu, F. (2023). Highly Secured Hybrid Image Steganography with an Improved Key Generation and Exchange for One-Time-Pad Encryption Method. AfyonKocatepe University Journal of Sciences and Engineering.
15. Senthilnayaki, B., Venkatalakshami, K., Dharanyadevi, P., G, N., & Devi, A. (2022). An Efficient Medical Image Encryption Using Magic Square and PSO. 2022 International Conference on Smart Technologies and Systems for Next Generation Computing (ICSTSN), 1-5.
16. Shankar, K., & Eswaran, P. (2016). An Efficient Image Encryption Technique Based on Optimized Key Generation in ECC Using Genetic Algorithm.