Image Encryption using Convolutional Neural Network

Subhashini K , Aarthi Lakshmi R, Arthi V, Hemalatha G
Sri Sairam Engineering College, ECE Department, Chennai, India

Abstract. The use of cryptography has become increasingly important in the transmission of multimedia, such as digital images, text, audio, and video, to ensure secrecy, integrity, confidentiality, and prevent unauthorized access to sensitive information. While Chaos-based cryptosystems are not yet standardized like AES, DES, RSA, they have emerged as an active area of research in recent years and can provide additional security when used with standard public key cryptosystems. This project aims to implement an effective image encryption approach using a Chaos-based cryptosystem to overcome differential attacks. The system involves dividing the original image into parts and repositioning them to form the first level of encryption. The encryption process starts with generating a one-dimensional sequence using a logistic map, which is then multiplied by the maximum pixel value and subjected to bit-by-bit operation. The result is used to encrypt the image, which can be decrypted using the same process in reverse.

1 Introduction

The process of transforming an image into a form that is unreadable to anyone who does not have the decryption key is known as image encryption. This is a significant cycle for getting delicate pictures and forestalling unapproved admittance to them. Convolutional Neural Networks (CNNs) is frequently utilized in image processing tasks like object recognition and image classification. However, recent studies have demonstrated that CNNs can also be used to encrypt images. In CNN-based image encryption algorithms, the pixel values of the input image are scrambled.. The result of the convolutional layers is then gone through a nonlinear initiation capability to additional increment the intricacy of the encryption cycle. The fact that CNNs can be trained on large image datasets to produce highly secure encryption algorithms is the primary benefit of using them for image encryption. Encryption algorithms based on CNN are also quick and effective, making them suitable for real-time applications. The various CNN- based encryption algorithms, their advantages and disadvantages, and their potential applications in the field of image security are discussed in greater detail here. It compares the performance of various CNN-based encryption algorithms to other cutting- edge image encryption techniques in this section.

2. Literature Review

There are two steps in the proposed method. The encryption key is generated in the first step using DEA. DEA is utilized to assess the overall efficiencies of pixels in the picture and create a key that can be utilized to scramble the picture. The scrambled image is fed into a CNN for further encryption in the second step.

In order to guarantee the CNN's resistance to a variety of attacks, it is trained on a large dataset. The key awareness examination is performed to assess the effect of changes in the encryption key on the scrambled image[1].

This paper begins with an introduction to the concept of image encryption and the challenges associated with it, including the need for high security, low computational complexity, and resistance to various types of attacks. The creators then, at that point, give an outline of the various sorts of CNN-based picture encryption strategies, including change based and replacement based techniques, as well as their half and half blends. The advantages and limitations of each approach are discussed in detail, along with the various techniques used for CNN- based image encryption, such as deep CNN, residual CNN, and generative adversarial networks[2].

This paper explains about the proposed method which uses two different chaotic maps: one for the generation of initial keys and the other for the pixel shuffling process.The encryption process starts with generating the initial keys using the first chaotic map. The keys are then used to generate a sequence of random numbers that are XORed with the original image to produce a new sequence of numbers. The encrypted image is then created by shuffle the pixel values of the new sequence using the second chaotic map. The decryption procedure employs the same two chaotic maps for both the generation of the initial keys and the reversal of the pixel values[3].

3. Existing Solution

Picture encryption is a significant field of study, especially with the rising utilization of profound learning calculations to upgrade the security of pictures.In medical imaging, the Internet of Medical Things, or IoMT, is frequently used to connect multiple images of the human body to create a complete picture for medical treatment.Researchers have used deep convolutional neural networks (CNNs) for image encryption to improve the robustness of 2D and 3D optical images to protect their privacy and security.Under deep residual networks, using various encryption keys to improve the accuracy of encrypted images is one method of image encryption. Deep neural networks can also be used to encrypt image pixels within positions, taking into account data augmentation, by grouping them into groups and simultaneously updating the key. By forestalling overfitting and upgrading the organization's speculation, this adds to an improvement in the exactness of the encoded pictures. Another technique for encrypting images is chaos-based deep learning image encryption. To create a safe encryption method, this strategy focuses on extracting low-dimensional features from the behavior of the pixels. Be that as it may, this approach is helpless against assaults, which is the reason analysts proceed to examine and foster new strategies for picture encryption utilizing profound learning. In general, deep learning-based image encryption is a complicated and difficult field of study that necessitates ongoing research and development to enhance the security and accuracy of encrypted images. It is essential to ensure that patient data is protected and secure from unauthorized access and attacks in light of the growing use of medical imaging and the IoMT.

4. Proposed Solution

Lately, as a rising number of organizations endeavor to store their information in a unified area for straightforward administration and access. However, security is a major concern, as it is with any system that involves the transmission and storage of sensitive data. To address this worry, analysts have been investigating different calculations and strategies for encoding information put away in nearby cloud frameworks. Using a hybrid algorithm that combines the encryption methods of chaos and convolutional neural network (CNN) is one promising strategy. An additional layer of security is provided by the use of a convolutional neural network as the initial encryption method in this strategy. Convolutional-based algorithms' encryption process is known to be complicated and hard to break, protecting against potential data breaches even further. After that, CNN-based encryption is used to further protect the encrypted data. This approach is probabilistic, implying that a solitary plain image can be scrambled into various conceivable code pictures, making it more moving for programmers to decode the information.

In general, the hybrid algorithm approach is a reliable and safe option for businesses that want to safeguard sensitive data. The algorithm can assist in the prevention of data breaches and ensure that confidential data remains protected from unauthorized access by combining chaos encryption with CNN encryption. While the hybrid algorithm offers high levels of security, it can be computationally demanding, requiring a lot of processing power to encrypt and decrypt data. Also, the calculation's effectiveness can be impacted by variables, for example, the size of the plain picture and the strength of the key utilized. In conclusion,businesses looking to protect sensitive data stored in local cloud systems may find the hybrid algorithm approach to be a promising option. The algorithm is able to provide high levels of security while maintaining the efficiency of the data transfer and storage processes by combining the advantages of chaos encryption and CNN-based encryption.

5. FLOW CHART

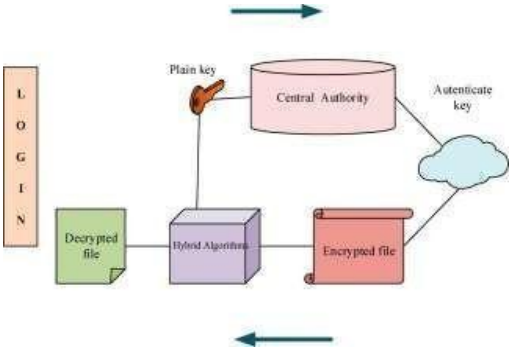


Fig. 5.1. Process Diagram of CNN

The novel approach to data encryption that you're referring to is a local cloud system-specific algorithm. Instead of being provided by a third-party service provider, local cloud systems are computing environments that are owned and operated by a single organization or individual. Encryption is an essential part of the security infrastructure of these systems because they frequently contain sensitive data that must be protected from unauthorized access. From the original plain image, the algorithm generates a variety of cipher images by employing a probabilistic convolutional neural network (CNN)-based encryption technique. The ability of CNNs,an artificial neural network, to process image data makes them ideal for this kind of encryption technique. Multiple cipher pictures with slightly different encryption keys can be created from the same plain image due to the probabilistic nature of the encryption method.

Since attackers cannot easily determine which image is identical to the original plain image, they have difficulty deciphering the encrypted data. The plain image is first broken up into smaller data "blocks" by the algorithm. After that, a CNN- based encryption technique is used to encrypt each block, resulting in a cipher picture. The cloud storage system receives the cipher images and stores them alongside the original plain image. At the point when the information should be gotten to once more, the code pictures are recovered from the distributed storage framework and decoded once again into the first plain picture. In general, this algorithm represents a promising strategy for encrypting data in local cloud systems.It is extremely secure because it employs a probabilistic CNN-based encryption technique, and its capacity to generate a variety of cipher pictures provides an additional layer of defense against intruders. Algorithms like this one will grow in importance as local cloud systems continue to gain popularity for protecting sensitive data stored in these environments.

Architecture on CNN:

A CNN's fundamental component is the convolutional layer.It extracts relevant features from the input image by applying a set of filters. In order to produce a single feature map, each filter is a compact matrix of learnable weight that is convolved with the input image. The channels are gotten the hang of during the preparation cycle utilizing back propagation.

The convolutional layer's receptive field is determined by the filter's size. More global features are captured by filters with larger sizes, while more local features are captured by filters with smaller sizes. The number of filters in a convolutional layer determines the number of feature maps produced. The result of the convolutional layer is gone through an actuation capability like the Corrected Straight Unit (ReLU) to bring nonlinearity into the organization.

Layer for Pooling:

The pooling layer is utilized to down sample the result of the convolutional layer. Max pooling, which selects the maximum value within a pooling window, is the most common pooling operation. This diminishes the spatial components of the element maps while protecting the most important highlights. L2 pooling and average pooling are two other pooling operations that can be used. There are many advantages to the pooling layer.To begin, it reduces the network's parameter count, which may assist in preventing overfitting. Second, it reduces the spatial dimensions of the feature maps, making the network more computationally efficient. Last but not least, it aids in introducing translation invariance into the network, which enables it to recognize objects regardless of where they are located in the image.

Completely Associated Layer:

The convolutional and pooling layers' outputs are processed by the fully connected layer in order to generate the final output. Every neuron in the preceding layer is connected to every neuron in the fully connected layer. This layer is used to complete the final classification or regression task.The purpose of the fully connected layer is to record the input data's high-level semantics.It tends to be considered a worldwide pooling activity that totals the elements across the whole picture. A softmax function is used to run the fully connected layer's output through to generate a probability distribution of the output classes.

CNN applications include:

For a wide range of computer vision problems, CNNs have become a popular algorithm. The following are some of the most common uses for CNNs:

Classification of Images:

In image classification tasks, where the objective is to classify an input image into one of several predefined categories, CNNs can be utilized. Instances of picture characterization assignments incorporate perceiving manually written digits, grouping various types of plants or creatures, and identifying various kinds of items in pictures.

Detection of Objects:

The goal of object detection tasks is to determine the presence and location of objects in an image using CNNs. Since object detection requires both recognizing an object's presence and locating it in the image, it is a more difficult problem than image classification.CNN-based encryption algorithms to other cutting- edge image encryption techniques in this section.

Segmentation of Images:

When dividing an input image into several regions, each of which corresponds to a distinct object or background, image segmentation tasks can be performed using CNNs. Because it is necessary to precisely identify the boundaries of various objects in the image, image segmentation is a more fine-grained task than object detection. The structure of a neural network is called its architecture. A neural network is made up of layers of neurons, or nodes, that are connected to each other and work together to process input data and make predictions about what will happen next. Neural networks, which are utilized in a wide range of fields like natural language processing (NLP), predictive modeling, and image and speech recognition, are inspired by the structure and function of the human brain.

The fundamental component of a neural network is the neuron. It processes the input values with an activation function to generate an output value. The layers of neurons that make up a neural network are an input layer, one or more hidden layers, and an output layer. Each layer is made up of a collection of neurons who work together to transform the input data and make predictions about the output.

A neural network's input layer is in charge of transferring input data to the first hidden layer. The quantity of information factors in the dataset decides the quantity of neurons in the information layer. The input layer, for instance, would have 784 neurons if the images in the input data were 28x28 pixels. A neural network's hidden layers are in charge of transforming the input data into a meaningful set of features that can be used to make predictions about the output. Hyperparameters that can be adjusted for optimal performance include the number of neurons in each secret layer and the number of secret layers. How each hidden layer neuron processes input data and generates output values is determined by its activation function.

A neural network's output layer is in charge of makin predictions based on the transformed input data. The quantity of neurons in the result not set in stone by the quantity of result factors in the dataset. For instance, the output layer would be comprised of ten neurons if the objective was to predict the probability that a given image falls into one of ten distinct classes.

Some of the architectures of neural networks include autoencoders, recurrent neural networks (RNNs), feedforward neural networks, and convolutional neural networks (CNNs).

A type of neural network called convolutional neural networks (CNNs) are made to process and analyze images. Convolutional layers, which are made up of filters that can learn to recognize particular image features like edges, textures, and patterns, are used in CNNs. CNNs are generally utilized in PC vision applications, like picture order, object recognition, and division. Recurrent neural networks (RNNs), a type of neural network, are designed to process data sequences, such as natural language or time-series data. RNNs can learn from the temporal dependencies and patterns in data by passing information from one time step to the next using a feedback loop.

A type of neural network called an auto encoder is made for unsupervised learning. An encoder network compresses the input data into a low-dimensional representation for auto encoders, and a decoder network uses the compressed representation to reconstruct the original input data.

Dimensionality reduction, feature extraction, and anomaly detection are all applications of auto encoders. The structure of a neural network, which consists of layers of interconnected neurons that collaborate to process input data and generate output predictions, is known as neural network architecture.

A neural network's architecture can be tailored to meet the requirements of a specific application, and various neural network types are utilized for various tasks.

6. RESULTS

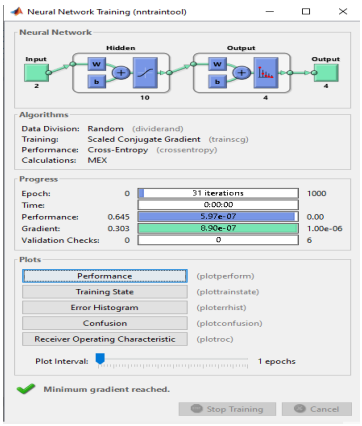
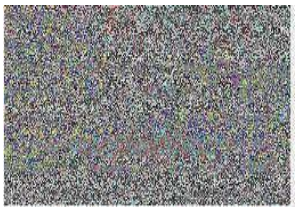
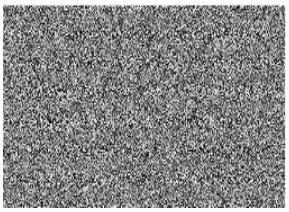
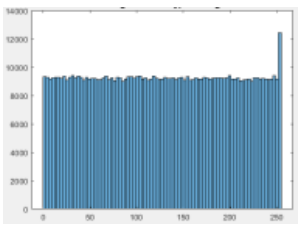
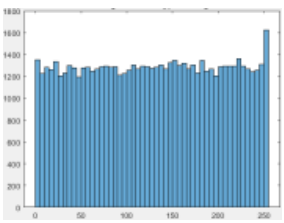
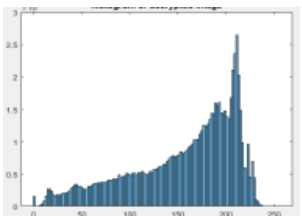
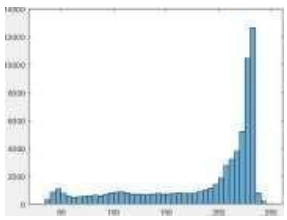
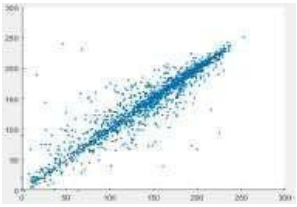
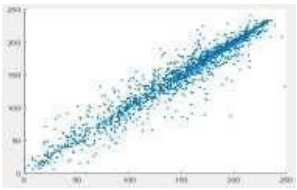
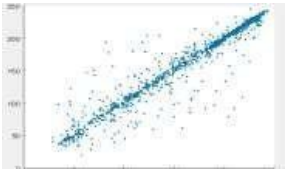
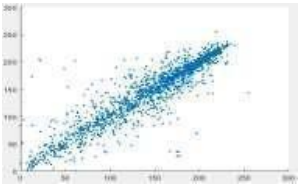
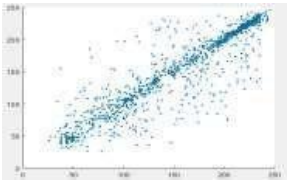
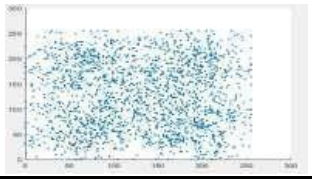
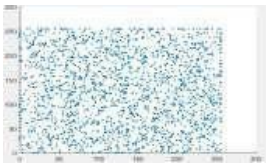
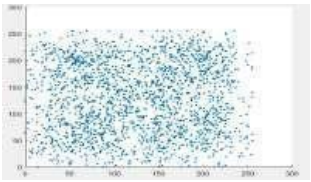
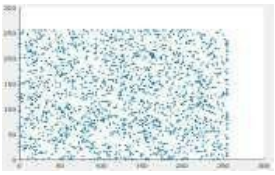
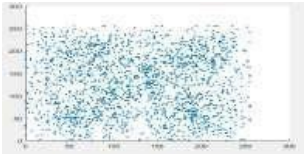
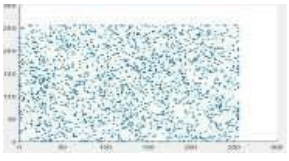


Fig. 6.1. Convolutional Neural Network for Clock Image

TABLE I

INPUT IMAGE		
ENCRYPTED IMAGE		
DECRYPTED IMAGE		
HISTOGRAM OF ENCRYPTED IMAGE		
HISTOGRAM OF DECRYPTED IMAGE		

HORIZONTAL CORRELATION OF PLAIN IMAGE		
VERTICAL CORRELATION OF PLAIN IMAGE		
DIAGONAL CORRELATION OF PLAIN IMAGE		
HORIZONTAL CORRELATION OF CIPHER IMAGE		
VERTICAL CORRELATION OF CIPHER IMAGE		
DIAGONAL CORRELATION OF CIPHER IMAGE		

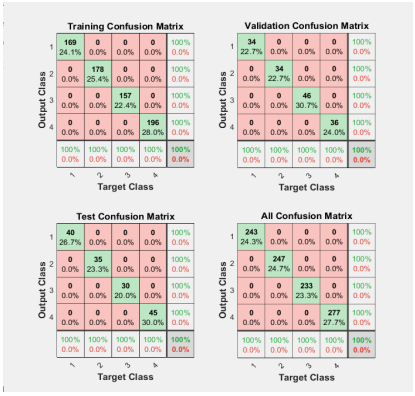


Fig. 6.2. Confusion Matrix of Clock Image

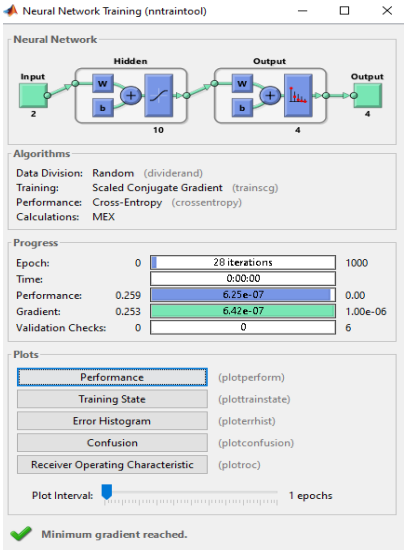


Fig. 6.3. Convolutional Neural Network of Car Image

A confusion matrix is a table that is often used to evaluate the performance of a machine learning model. It summarizes the counts of true positives, true negatives, false positives, and false negatives for a given classification problem. In the context of image encryption, a confusion matrix can be used to evaluate the performance of an encryption algorithm. Here's an example of what a confusion matrix might look like for an image encryption model:

Table 6.1. Confusion Matrix

	Predicted Positive	Predicted Negative
Actual Positive	True Positive (TP)	False Negative (FN)
Actual Negative	False Positive (FP)	True Negative (TN)

The terms positive and negative refer to whether an image has been encrypted or not. A true positive (TP) occurs when an image is correctly identified as encrypted, while a false negative (FN) occurs when an encrypted image is incorrectly classified as not encrypted. Similarly, a true negative (TN) occurs when an image is correctly identified as not encrypted, while a false positive (FP) occurs when a non-encrypted image is incorrectly classified as encrypted.

Fig. 6.4. Confusion Matrix for House Image

7. CONCLUSION

Convolutional based calculations encryption interaction is known to complex and difficult to break, providing an additional level of protection against data breaches. The encrypted data is then further secured with CNN-based encryption. Since a single Plain image can be encrypted into multiple cipher images, hackers will have a harder time decrypting the data using this probabilistic approach**.**

REFERENCES

[1] V. Kakkad, M. Patel, and M. Shah, "Biometric authentication and image encryption for image security in cloud framework," Multiscale and Multidisciplinary Modeling, Experiments and Design, vol. 2, no. **4**, pp. 233–248(2019)**.**

[2] Z. Hua, B. Xu, F. Jin, and H. Huang, "Image encryption using Josephus problem and filtering diffusion," IEEE Access, vol. **7**, pp. 8660–8674(2019).

[3] S. R. Maniyath and V.anikaiselvan, "An efficient image encryption using deep neural network and chaotic map,"Microprocessors and Microsystems, vol. **77**, Article ID 103134(2020).

[4] Y. Ding, "DeepEDN: a deep learning-based image encryption and decryption network for internet of medical things," IEEE Internet of ings Journal, vol. **8**, no. 3, pp. 1504–1518(2020).

[5] S. Yadav and N. Tiwari, "Recent advancements in chaos-based image encryption techniques: a review," SocialNetworking and Computational Intelligence, Springer, Singapore, pp. 639–647(2020).