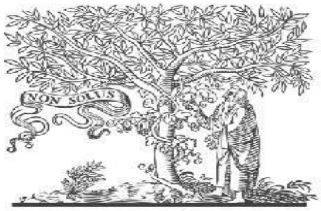
International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

COPY RIGHT



ELSEVIER SSRN

IJIEMR Transactions, online available on 10th Apr 2023. Link :http://www.ijiemr.org/downloads.php?vol=Volume-12&issue=Issue 04

10.48047/IJIEMR/V12/ISSUE 04/50

Title **Encryption and Decryption of images through ANN Using MATLAB**

Volume 12, ISSUE 04, Pages: 419-426

Paper Authors

Mr.K.Rasululla, P.Susmitha, K.Sai Javali, P.N.M.Kathyayani, V.Vinay Kumar

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

Encryption and Decryption of images through ANN Using MATLAB

Mr.K.Rasululla,M.Tech(Ph.d),Associate professor Department of EEE,
Vasireddy Venkatadri Institute of Technology, Nambur, Guntur Dt., Andhra Pradesh.

P.Susmitha, **K.Sai Javali**, **P.N.M.Kathyayani**, **V.Vinay Kumar**
UG Students, Department of EEE,
Vasireddy Venkatadri Institute of Technology, Nambur, Guntur Dt., Andhra Pradesh.
shaikrasool@vvit.net

Abstract

This article proposes an encryption image algorithm possibly called the stream of modified Image Encryption to verify secure image transmission requests. This algorithm is based on the symmetric key encryption method. The system uses a neural network (NN) based pseudo-random number generator with back-propagation learning algorithm. This will provide the necessary nonlinear properties that increase the statistical properties of the pseudo-random generator randomness. The results of the computer simulation based on the MATLAB simulation were performed to demonstrate the effectiveness of the learning process to obtain the effective weights. The results also show several experimental and statistical analyzes to demonstrate the randomness of the pseudo-random generator as well as the proposed image encoding and decoding. The result reflects a simple and effective image security system.

Keywords: Image encryption, Image decryption, Neural network, Stream cipher.

Introduction

Over the past decade, there has been considerable advancement in Internet and multimedia technologies, which has resulted in the widespread usage of digital pictures as essential carriers of information transmission for individuals. Enforcing security and assuring authorised access to sensitive data has been the principal impediment to the broad implementation of digital picture services. The employment of an encryption technique to hide the visual data streams is a straightforward solution to this issue. The issue of image protection has existed since the dawn of information technology. Picture is a multimedia signal that provides a guy with the greatest information. Vision perception accounts for more than 80% of information. It is the primary reason for safeguarding a picture against unauthorised viewing. A stream cypher is made out of Pseudo-Random Number

Generators (PRNG). For encryption, a PRNG is started with a key and offers its output as a series of bits greater than the current pseudo-key. The chance is critical because it entirely undermines the statistical features of the message. Using linear feedback shift registers to generate current keys (LFSR). The LFSR approach attempts to imitate a one-time pad by generating a lengthy line of critical information. As with any such endeavour, cracking a section of the cryptogram cryptanalyst reveals information about other parts of the cypher text when the key is shorter than the message itself. Parts of the key sequence for an LFSR, a known-plaintext attack (Akhil et al, 2011). In general, an XOR gate combines the key stream (XOR) with a piece of text. To decipher the message bit encryption text is XORed with the appropriate bit sequence once more. A flaw in a single encrypted bit mistake in plain text. This is especially handy if the transmission error rate is high (A. Menezes et al, 1996).

The one-time pad is a stream cypher that has been demonstrated to be secure. In this diagram. Each character key is produced at random and is only used once.

PROCESS OF IMAGE ENCRYPTION AND METHODOLOGY

Cryptography is the science of turning information in readable format into a format that others cannot read, i.e. the science of information security. Given the dizzying speed of today's technology, the security gap faced by new technologies becomes more significant. Image security has become increasingly crucial in today's digital environment issue. To provide this security, encryption is utilised. The science of encryption is known as cryptology. Encryption is used to protect data.

There are several neural network-based picture encryption techniques, such as:

1.Algorithms based on Convolutional Neural Networks (CNN): These techniques employ a deep neural network architecture tailored exclusively for image processing. The CNN model takes the original image as input and outputs an encrypted image.

2.Algorithms based on auto encoders: Auto encoder models are neural networks that are meant to learn a compressed version of the input data. In picture encryption, an auto encoder can be used to compress the original image, which can then be encrypted using typical encryption techniques.

3.Algorithms based on Generative Adversarial Networks (GAN): GANs are a form of neural network has two models, one for the generator and one for the discriminator. The generator may be taught to produce an encrypted version of the original picture in image encryption,

while the discriminator is used to assess the quality of resulting image.

Overall, neural network-based picture encryption methods have the potential to be more secure and efficient than classic encryption techniques. However, its efficiency will be determined by factors such as the network architecture's complexity and the quality of the training data utilised to train the model.

System Implementation

The following steps are commonly included in the system implementation of picture encryption using neural networks:

1.The original picture is initially preprocessed to ensure that it is in a format acceptable for input into the neural network. It may be necessary to resize the image to a specified size or to normalise the pixel values to a specific range.

2.Developing the neural network architecture for picture encryption: The next stage is to build the neural network architecture for image encryption. This may entail using an existing architecture or creating a bespoke architecture customized to the application's unique requirements.

3. When the architecture has been determined, the neural network is trained using a dataset of input-output pairs. The input data consists of a collection of unencrypted photographs, while the output data consists of the encrypted versions of those images. Using a loss function, the network is trained to minimize the difference between the output and target pictures.

4.Creating the encryption key: When the neural network has been trained, an encryption key is created. This key is used to encrypt the original picture by performing a series of mathematical operations on the image's pixel values. A secure random number generator is often used to produce the encryption key.

5. Decrypting the picture: The same neural network is used in reverse to decode the encrypted image. The encrypted picture, together with the decryption key, is sent across the network. The original, unencrypted picture is then generated by the network.

6.Lastly, the system is tested and verified to confirm that it is functioning properly. This may entail testing the system on a number of distinct pictures and assessing its performance in terms of encryption speed, security, and decryption accuracy.

Generally, image encryption system implementation employing neural networks necessitates a mix of skills in image processing, machine learning, and cryptography. The system's efficacy will be determined by the quality of the neural

network design, training data, and encryption key generation technique utilised.

Prerequisites

Before implementing picture encryption using neural networks, certain criteria must be met. These are some examples:

1.Knowledge of image processing: To preprocess pictures before feeding them into the neural network, a thorough grasp of image processing is required. This covers procedures like scaling, normalization, and data augmentation.

2.Experience with neural networks: Understanding neural network architecture and design is required to develop picture encryption using neural networks. This covers understanding of different layers, activation functions, loss functions, and optimization strategies.

3. Availability to acceptable datasets: It is critical to have access to a suitable dataset of unencrypted and encrypted picture pairings while training a neural network for image encryption. This dataset should be large enough to give enough variation in the input pictures while being computationally practical for training the network.

4.Cryptography knowledge: A solid grasp of cryptography is required to create a safe and efficient encryption scheme. Knowledge of symmetric and asymmetric key encryption, block and stream cyphers, and cryptographic hash functions is required.

5. Picture encryption with neural networks may be computationally costly, especially when dealing with huge datasets or complicated neural network topologies. To accomplish appropriate training and inference times, enough computational resources, such as GPUs or cloud-based computing, may be required.

6.When implementing picture encryption using neural networks, it is critical to be cognizant of ethical factors such as privacy concerns and the possibility of unforeseen effects. It is critical that the system is built and executed with an emphasis on ethical and social responsibility in mind.

Neural Network Algorithm

Deep neural networks are used in neural network encryption methods for image encryption to transform an input picture into an encrypted form that is difficult to read without the decryption key. The following are the fundamental processes of a neural network encryption technique for picture encryption:

1.The input picture is preprocessed to ensure that it is in a format appropriate for input into the neural network. It may be necessary to resize the image to a

specified size or to normalise the pixel values to a specific range. continues until there are no more points to add to this cluster.

2.Developing the neural network architecture for picture encryption: The next stage is to build the neural network architecture for image encryption. Many layers of convolutional and pooling procedures are often followed by fully linked layers in the architecture. Depending on the complexity of the picture data and the security requirements, the number of layers and the size of each layer may vary.

3.When the architecture has been determined, the neural network is trained using a dataset of input-output pairs. The input data consists of a collection of unencrypted photographs, while the output data consists of the encrypted versions of those images. Using a loss function, the network is trained to minimise the difference between the output and target pictures.

4.Decryption: The same neural network weights are employed in reverse to turn the encrypted pixel values back into the original picture to decode an encrypted image. This necessitates knowledge of the right decryption key, which might be a secret key shared by the sender and recipient or a public key used in a public-key encryption system.

Overall, because the encryption process is based on complicated mathematical functions that are difficult to reverse-engineer without knowledge of the neural network weights and decryption key, neural network encryption methods can provide a high level of security and resilience to assaults. These algorithms, however, can be computationally demanding and may necessitate large resources to train and implement.

Implementation of Image Encryption

Here's an outline of how neural networks may be used to perform picture encryption:

1.Data preprocessing: Import the visual data and transform it to a numerical representation that a neural network can process. Converting the picture to grayscale or RGB format, scaling the image to a specific dimension, and normalising the pixel values to a range between 0 and 1 are all examples of this.

2.Neural network architecture: Create a neural network architecture capable of encoding and decoding picture data. This may entail utilising convolutional layers to extract picture information and fully linked layers to do encoding and decoding.

3.Training the neural network: Train the neural network with a large number of training images and a loss function that

compares the original and encoded images. The objective is to discover a set of weights that can encode and decode pictures properly.

4.To encrypt a picture, send it through the trained neural network and output the encoded image. The encoded picture can then be further encrypted with a conventional encryption method like AES or RSA. The generated ciphertext can be safely sent or stored.

5.Image decryption: To decrypt an encrypted picture, first decrypt the ciphertext with the standard encryption technique, and then decode the resultant image with the trained neural network. The picture may then be encrypted and rebuilt in its original format.

Overall, image encryption using neural networks can provide a high level of security and robustness because the neural network can learn complex mappings between the original and encoded image data that are difficult to reverse-engineer without knowledge of the neural network weights and decryption key. Nevertheless, constructing and training the neural network may be time-consuming and computationally costly.

Case Study

Jiang et al. (2019) introduced a deep neural network-based picture encryption technique that combines a convolutional neural network (CNN) with a feedback shift register (FSR) encryption algorithm, which is a major case study of image encryption utilising neural networks.

The CNN algorithm is used to extract high-level characteristics from the input picture, which are subsequently encrypted using the FSR method to generate ciphertext. The FSR encryption is reversed and the resultant ciphertext is sent through the CNN to reconstruct the original picture.

The authors tested their image encryption scheme on several benchmark datasets, including the industry-standard MNIST and CIFAR-10 datasets, and discovered that it achieved high levels of security and robustness against various attacks, such as differential attacks, brute-force attacks, and model-based attacks.

This method of picture encryption offers a fresh solution by combining the strengths of neural networks with classic encryption techniques. It also highlights the power of deep learning techniques in the realm of cryptography, revealing new avenues for safe and efficient data encryption.

FUTURE SCOPE:

The future scope of the encryption and decryption where in other words also called as cryptography is QUANTUM COMPUTING.Expect Double Exponential Growth via Quantum Computing

Classical computing uses electrical signals to encode data in bits. Each bit

can have a value of 0 or 1. Quantum computing can use other physical systems, such as electrons and protons, to encode data in qubits. A qubit can have a state of 0, 1 or some combination of those digits. Because the quantum state of a qubit can be almost infinite, a qubit can encode exponentially more data than a bit.

Classical computing performance has experienced exponential growth, increasing by powers of 2 (2, 4, 8, 16, etc.). Quantum computing is expected to involve double exponential growth, increasing by powers of powers of 2 (4, 16, 256, 65,536, etc.). You can see how quickly the performance of quantum computers will leap ahead.

Making Encryption Harder, Better, Faster and Stronger

In response, the industry is advancing encryption on several fronts. Some efforts are focused on increasing key sizes to protect against brute-force decryption. Other efforts are looking at new cryptographic algorithms. For example, the National Institute of Standards and Technology is evaluating a next-generation public key algorithm intended to be quantum safe.

Conclusion

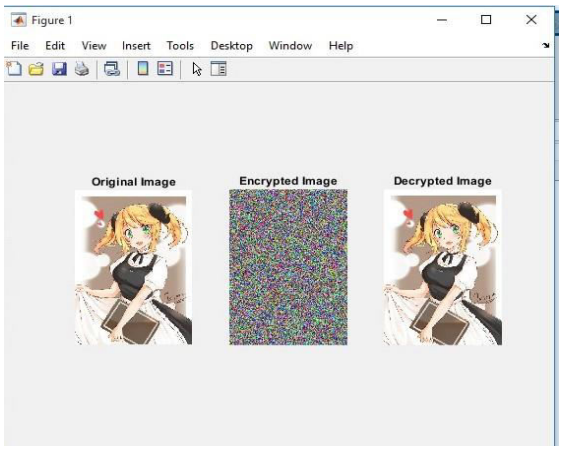
In this article, Finally, picture encryption using neural networks is a promising solution that provides high levels of security and robustness against a variety of assaults. By encoding and decoding picture data with neural networks, it is feasible to generate complicated and non-linear mappings between the original and encrypted data that are difficult to reverse-engineer without knowledge of the neural network weights and decryption key.

While this strategy has advantages, it also has drawbacks. Building and training a neural network for picture encryption may be time-consuming and computationally expensive, needing significant quantities of data and computing power. Moreover, the security of neural network-based encryption methods may be influenced by the encryption key's quality as well as the security of the underlying hardware and software systems.

Overall, picture encryption using neural networks is an attractive field of study that has the potential to improve image data security and privacy in a range of applications such as medical imaging, satellite images, and video surveillance.

As research in this field advances, we should expect to see new and inventive ways to picture encryption that take advantage of neural networks' particular strengths.

Output



References

[1] Chin-Chen Chang, Min-Shian Hwang, Tung-Shou Chen, "A new encription algorithm for image cryptosystems", The Journal of Systems and Software, 22 August 2000.

[2] Rasul Enayatifar, Abdul Hanan Abdullah, "Image Security via Genetic Algorithm", International Conference on Computer and Software Modeling IPCSIT vol.14, 2011

[3] Ravindra Gupta, Akanksha Jain, "Integrating Steganography Using Genetic Algorithm and Visual Cryptography for Robust Encryption in Computer Forensics", International Journal of Electronics and Computer Science Engineering, 2012

[4] Sandeep Bhowmik, Sriyankar Acharyya, "Image Cryptography: The Genetic Algorithm Approach", Computer Science and Automation Engineering (CSAE), 2011 IEEE International Conference

[5] Güvenoğlu E., "Görüntü Şifrele Algoritmaları ve Performans Analizleri", Yüksek Lisans Tezi, 2006

[6] J.Park,I.W. Sandberg, Universal Approximation Using Radial Basis Function Networks, Neural Computation, Cilt 3, 246- 257, 1991.