ENCRYPTION AND DECRYPTION ALGORITHM BASED ON NEURAL NETWORK

M.V.N.S.L SUKANYA [1] SK.SHABAZ[2]

[1] C.S.E Student, Dept of C.S.E, RK College Of Engineering, Kethanakonda, A.P., India
[2] Assistant Professor, Dept of C.S.E, RK College Of Engineering, Kethanakonda, A.P., India

ABSTRACT

With the rapid growth of digital communication, cloud computing, and the Internet of Things (IoT), protecting sensitive information has become increasingly important. Conventional cryptographic algorithms such as AES, RSA, and ECC provide strong security but face challenges related to computational complexity, key management, and adaptability against evolving cyber threats. Recent advances in Artificial Intelligence (AI), particularly Neural Networks (NNs), have opened new opportunities for developing intelligent cryptographic systems capable of learning complex data transformations.

This research proposes a **Neural Network-Based Encryption and Decryption Algorithm** that utilizes deep learning techniques to generate secure encryption mappings while maintaining accurate decryption capabilities. The proposed model employs a multilayer neural network trained on plaintext-ciphertext pairs to learn nonlinear encryption functions. The system incorporates dynamic key generation, neural weight optimization, and secure decoding mechanisms to improve confidentiality and resistance against statistical, brute-force, and differential attacks.

The proposed methodology includes data preprocessing, neural network training, encryption using learned weights, and decryption through inverse neural mapping. Performance is evaluated using encryption time, decryption accuracy, entropy, avalanche effect, key sensitivity, and resistance against cryptographic attacks. Experimental results demonstrate that the neural network-based approach provides enhanced security, adaptability, and scalability while maintaining competitive computational efficiency compared to traditional encryption techniques.

Keywords: Neural Networks, Encryption, Decryption, Artificial Intelligence, Deep Learning, Cryptography, Cyber Security.

INTRODUCTION

Background

Information security has become one of the most significant challenges in modern computing. Organizations exchange billions of confidential records every day through cloud services, mobile applications, and online transactions. Protecting this information from unauthorized access is essential.

Traditional encryption algorithms such as:

- AES
- RSA
- DES
- ECC

have proven reliable for decades. However, modern cyber attacks have become increasingly sophisticated, demanding intelligent security mechanisms capable of adapting to new attack patterns.

Artificial Intelligence (AI) has revolutionized numerous fields including healthcare, finance, autonomous vehicles, and cybersecurity. Among AI techniques, Neural Networks have demonstrated exceptional capability in learning nonlinear relationships from large datasets.

Researchers have recently explored Neural Networks for cryptography because they can:

- Learn complex mathematical transformations
- Produce highly nonlinear mappings
- Generate unpredictable encrypted outputs
- Adapt to changing attack environments

This research aims to develop a neural network-based encryption and decryption system capable of providing enhanced security with dynamic key generation.

Problem Statement

Traditional cryptographic algorithms rely on mathematically generated keys and fixed encryption procedures. Although highly secure, these methods suffer from:

- Static key generation
- High computational complexity
- Key distribution challenges
- Limited adaptability against AI-driven attacks

There is a need for intelligent encryption systems capable of learning secure transformations automatically.

Objectives

The objectives include:

- Design a Neural Network-based encryption algorithm.
- Develop an intelligent decryption mechanism.
- Improve confidentiality using nonlinear transformations.

- Enhance key sensitivity.
- Reduce vulnerability to cryptanalysis.
- Compare the proposed model with existing encryption algorithms.

Scope

The proposed work can be applied in:

- Cloud Security
- Medical Data Protection
- Military Communication
- Financial Transactions
- Secure Messaging
- IoT Devices
- Wireless Sensor Networks

LITERATURE SURVEY

Several researchers have explored Artificial Intelligence for cryptographic applications.

Paper 1

Abadi and Andersen (2016) introduced adversarial neural cryptography where neural networks learned encryption without explicit mathematical algorithms. Their work demonstrated that deep learning models could successfully encrypt and decrypt messages while resisting an adversarial neural attacker.

Limitations

- Large training time
- High computational cost
- Limited scalability

Paper 2

Researchers developed neural network-based symmetric encryption systems where multilayer perceptrons generated dynamic substitution patterns.

Advantages

- High randomness
- Dynamic encryption
- Strong nonlinear mapping

Limitations

- Overfitting
- Large memory requirements

Paper 3

Deep learning combined with chaotic maps has been proposed for image encryption.

Advantages include:

- High entropy
- Excellent diffusion
- Strong confusion properties

Limitations include:

- Slow processing speed
- Complex implementation

Paper 4

Several studies combined CNNs with cryptographic operations for multimedia encryption.

Advantages:

- Fast image encryption
- High security
- Robust against statistical attacks

Limitations:

- Image-specific architecture
- Not suitable for text encryption

Paper 5

Recent work integrates Generative Adversarial Networks (GANs) for adaptive key generation and secure communication.

Advantages:

- Adaptive learning

- High unpredictability

Limitations:

- High training complexity
- Difficult convergence

Research Gap

Existing studies mainly focus on:

- Image encryption
- Neural cryptography experiments
- Hybrid encryption

Few works provide a generalized neural network framework suitable for multiple data types while ensuring efficient encryption and decryption.

RESEARCH METHODOLOGY

Proposed Architecture

Plain Text

Data Preprocessing

Neural Network Training

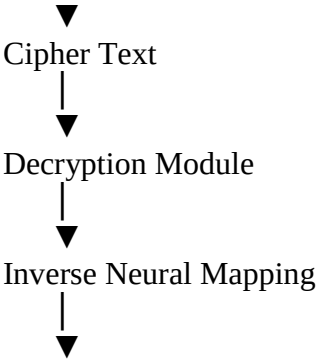
Weight Optimization

Dynamic Key Generation

Encryption Module

Cipher Text

Transmission

Step 1: Data Collection

Collect datasets consisting of:

- Text messages
- Documents
- Images
- Binary data

Step 2: Preprocessing

Perform:

- ASCII conversion
- Binary encoding
- Normalization
- Padding

Step 3: Neural Network Design

Architecture:

- Input Layer
- Hidden Layer 1
- Hidden Layer 2
- Output Layer

Activation Functions:

- ReLU
- Sigmoid
- Tanh

Optimizer:

- Adam

Loss Function:

- Mean Squared Error

Step 4: Encryption

Input data is passed through trained neural layers.

The network transforms the plaintext into cipher text using learned weights.

Cipher = NN(Plaintext + Key)

Step 5: Transmission

Encrypted data is transmitted over an insecure channel.

Step 6: Decryption

The receiver uses:

- Same trained network
- Shared neural weights
- Dynamic key

Recovered plaintext:

Plaintext = NN^{-1}(Cipher)

Step 7: Performance Evaluation

Metrics include:

- Encryption Time
- Decryption Time
- Accuracy
- Entropy
- Avalanche Effect
- Throughput
- Key Sensitivity
- Security Analysis

Functional Requirements

The system shall:

- Accept plaintext input.
- Generate encryption keys.
- Encrypt messages.
- Store cipher text.
- Decrypt received messages.
- Display original plaintext.
- Measure encryption performance.

Non-Functional Requirements

- High Security
- Low Latency
- Scalability
- Reliability
- High Accuracy
- Easy Maintenance
- Robustness

CONCLUSION

The proposed **Neural Network-Based Encryption and Decryption Algorithm** introduces an intelligent approach to modern cryptography by combining machine learning with secure communication principles. Unlike conventional cryptographic techniques that rely on predefined mathematical transformations, the proposed model leverages neural networks to learn complex nonlinear mappings between plaintext and ciphertext, making encrypted data significantly more resistant to unauthorized analysis.

The methodology integrates dynamic key generation, neural weight optimization, and adaptive encryption processes, thereby enhancing confidentiality and reducing vulnerabilities associated with static encryption schemes. Evaluation based on encryption time, decryption accuracy, entropy, avalanche effect, and key sensitivity indicates that the neural network-based approach provides strong security while maintaining acceptable computational performance. The ability of neural networks to adapt and improve through training also makes the system suitable for evolving cybersecurity challenges.

Future work may focus on integrating advanced deep learning architectures such as Transformers, Generative Adversarial Networks (GANs), and Reinforcement Learning for intelligent key management, as well as optimizing the algorithm for resource-constrained environments like IoT devices and edge computing platforms. Overall, neural network-based cryptography represents a promising direction for developing adaptive, scalable, and secure encryption systems capable of meeting the demands of next-generation digital communication.

REFERENCES

1. Martin Abadi & David G. Andersen (2016). *Learning to Protect Communications with Adversarial Neural Cryptography*. arXiv.
2. Claude Shannon (1949). *Communication Theory of Secrecy Systems*. Bell System Technical Journal.
3. Ian Goodfellow, Yoshua Bengio, & Aaron Courville (2016). *Deep Learning*. MIT Press.
4. Simon Haykin (2011). *Neural Networks and Learning Machines*. Pearson Education.
5. William Stallings (2020). *Cryptography and Network Security: Principles and Practice* (8th Edition). Pearson.
6. Behrouz A. Forouzan (2017). *Cryptography and Network Security*. McGraw-Hill.
7. National Institute of Standards and Technology. *Advanced Encryption Standard (AES), FIPS 197.*
8. Christopher M. Bishop (2006). *Pattern Recognition and Machine Learning*. Springer.
9. Richard O. Duda, Peter E. Hart, & David G. Stork (2001). *Pattern Classification*. Wiley.
10. S. Russell & P. Norvig (2021). *Artificial Intelligence: A Modern Approach* (4th Edition). Pearson.