An analysis on the current researches in encryption algorithms based on neural networks

Jin Ouyang
School of Control and Computer Engineering, North China Electric Power University, Beijing, China
angela@cas-harbour.org

Abstract. To perform an in-depth analysis on the current researches concerning the application of neural networks in the encryption algorithms, this paper used some research methods such as literature review and algorithm analysis to review the proposal and application of neural network technologies as well as the proposal and research and development of encryption algorithms through. The importance of neural networks in the encryption algorithms is highlighted. The current researches on encryption algorithms based on neural networks are reviewed from three dimensions, namely, algorithm framework, algorithm model and algorithm application. Through the research, it shows that the neural network technology has become the preferred choice for developing the encryption algorithms. This paper also proposed the direction of improvement through fusion application of multiple information processing technologies. This work lays the basis for improving the encryption algorithms based on neural network.

1. Introduction
Along with the rapid development of the network information technology and the expansion of amount of information, query of more information on a certain person or object can be powered by the association between the information [1]. To protect individual privacy and important information on some items, a whole set of information protection scheme must be devised. At present, encryption serves as the main tool for information protection. As an important information processing technology, neural networks are frequently applied to the encryption algorithms. Here, the status quo of application of neural networks in encryption is summarized based on literature reviewed.

2. Studies on neural network
2.1 Proposal of the neural network technology
Human brain is an important tool for information recognition and storage and classifies information into different types, including graphical and textual information. This mechanism helps man learn new knowledge and expand the knowledge quantity. An analogy can be made between human brain and computer when it comes to the issue of information processing. [2] Both acquire the ability of problem analysis through information processing. As the amount of information grows, more information needs to be stored. However, the human brain, with limited storage space and lower information processing ability, does not support complex information processing. Given the memorizing ability of the brain, the memory points in the brain can be subject to systematic processing, followed by the extraction of more important information from a myriad of information, thus reducing the amount of information to...
be processed.

Pitts was the first to propose the concept of neural network in 1943, based on the study of the physiological features of neurons from the mathematical perspective. With the construction of the mathematical model of neurons, the era of artificial neural network thus began. After 14 years of in-depth investigation, F. Rosenblatt built a neural network-based sensor and applied it to the solving of some complex information analysis problems. In 1984, physicists put forward the design schemes for continuous and discrete networks. By the end of the 1980s, artificial neural network became a research hotspot. Now artificial neural networks have been applied to even a broader range of fields.

2.2 Application of neural networks
Neural networks open new pathways to information processing and analysis. At present, neural networks have been applied to information evaluation, speech recognition, information recognition and medical research. Among the application studies in information evaluation, the neural network is incorporated into a quantitative model and the study is designed by using an evaluation indicator system. A precise information evaluation is achieved through the refined design of neural network. As to the application studies in speech recognition, the recognition system is usually built based on the neural network learning rules and by combining with the speech recognition principles and learning mechanism of network. It is thus determined which working staff in the database the voice message comes from, so as to facilitate the recognition of the sender of the voice message.[3] Studies on information recognition are similar to those on speech recognition, except that the voice message are replaced by the text messages. Application studies in the medical field generally fit the treatment information into one database. Then a network is built based on the association between each piece of treatment information, which facilitates the traversal of information.

In addition to the above, neural networks have been also applied to information processing, such as encryption.

3. Studies on encryption algorithms

3.1 Proposal of the idea of encryption
Rapid progress being made in Internet technologies not only brings convenience for information query, but also brings information safety risks. A large amount of information is stolen and misused unknowingly, which causes a severe impact on personal life and company operation. Although the use of computer firewall has blocks some behaviors of information theft, information safety is still being threatened. Encrypted information, if even stolen, cannot be accessed in its right form, which helps protect the information. Therefore, encryption emerges in response to the urgent need for information protection in this era.

3.2 Encryption algorithm
A whole set of encryption algorithm is highly important for solving the problem of information theft. Many studies have been conducted on the encryption algorithms. Generally, the encryption algorithms are written based on information features, so as to increase the safety of information.

But because of the massiveness and diversity of information, it usually takes a large amount of time to process the data. There is also the problem of omission during data processing, thus threatening information safety. For example, the reorganization encryption technology disrupts the current pattern of information combination according to a certain sequence requirements. The wrong sequence can be only cracked using the accurate password to obtain the accurate information. This algorithm can save time, but during the cracking process, the problems of information missing and messy codes are likely to occur, which need to be further improved. The Hash algorithm, when applied to encryption, utilizes the information encrypted by the SHA1 and MD5 algorithms. Although the error rate of encryption is low, the algorithm development is difficult and a higher requirement is placed on the expertise of the algorithm development and application staff. That is why Hash algorithm is not so commonly used in
encryption \[4\].

The concept of neural network was first proposed in 1943. After many years of improvement, the neural network system has already matured, and lower technical requirements are placed on the users. The processing scheme is developed based on the basic neural network model and by combining with the requirements on information processing, and this approach has achieved a good application effect when applied to encryption. Therefore, the neural network technology has become the preferred choice for developing the encryption algorithms.

4. Studies on encryption algorithms based on neural networks

4.1 Proposition of the algorithm framework

According to the working principles of the neural network model and development requirements, this technology is of great help for encryption and considered one of the most important tools. Hence, the encryption algorithms based on neural networks have become an epidemic focus. The algorithm framework is built upon the neural network model and classifies the information into several types. Then the neural network system is constructed according to the relationship between information of each type and the algorithm framework structure is formed.

4.2 Construction of the algorithm model

Some other studies on algorithm models use the neural network as a system recognizer and design a control system for the encryption. For example, the neural network system is constructed based on the laws of dead-beat control and initial value control. The information structure is reconstructed by using the neural network system and the chaotic sequence is obtained. Next, the ciphertext is generated by replacing with plaintext, thus achieving the encryption \[5\]. In order to improve the safety of encryption, hierarchical encryption is proposed in some studies. Depending on extreme sensitivity, back propagation is usually introduced to form a multi-level safety hierarchy. If the safety level is too low, it is necessary to implement back propagation again depending on sensitivity, so as to reduce the error.

After that, the encryption scheme combining neural networks and hardware is proposed, where the neural network-based encryption algorithms are developed depending on hardware features and the encryption function is realized through the hardware \[6\]. For example, the neural network is incorporated into the STM32 single chip microcomputer to write the control algorithm, and then the acquired information is encrypted for confidentiality purpose \[7\]. So far, this encryption method has been applied to agricultural and industrial fields.

In fact, studies in the neural network-based encryption algorithms are closely related to information processing and may lay down the encryption algorithm research protocol from the perspective of data processing. For example, a function is introduced, and based on the features of this function, the data information is transformed into the information as represented by function features. Only the personnel who encrypt the information can understand the meaning of the encrypted data, thereby achieving the confidentiality purpose \[8\]. At present, studies on neural network-based encryption algorithms that involve function construction are mainly divided into image processing and encryption, information processing and encryption, digital watermark encryption, and differential attack for chip encryption.

Information processing and encryption technology is an information transcoding technology. That is to say, the information to be encrypted is transcoded depending on the features of a specific function and then substituted into the function framework to obtain new values. This method disrupts the original information structure and alters the meaning of information. If this transcoded information is stolen, it is needless to worry about information exposure. The information transcoding process is simple and safe, and it is therefore highly favored and frequently used in information processing. The current studies on information transcoding usually start from the function structure and improve it from simple to complex based on the demands of information encryption. All that need to be done is to substitute the function during the encryption, after which the system will automatically generate the
encrypted information. In that case, the function should be reconstructed. Generally, this encryption method has a bright application prospect, while function structure construction requires further investigation.

Digital watermark encryption is a combination of the watermark technology and neural networks, and watermarks are added depending on network deployment to achieve the confidentiality purpose. Generally speaking, the digital watermark technology is more frequently used in paper publication. To avoid plagiarism, watermarks are added to the center of the page or to the pictures to cover up some important information. Or, identification is added to the papers to prove that this paper is created by the specific author, thus protecting the intellectual property rights. The digital watermark technology is being used more widely. In addition to the paper publication platforms such as CNKI and Wanfang, this technology can be also applied to the papers uploaded to Baidu and Doc88, which is of great help to protect the intellectual property rights.

Differential attack for chip encryption refers to the construction of differential function by utilizing the chip. The information is processed to generate new information and to increase the difficulty of information discrimination, thus raising the level of encryption. In actual practice, information input, as controlled by the chip, is processed by the function to obtain new information. Comparison of the new information and original information shows that the meaning of the new information after differential processing is very much unlike that of the original information. Therefore, information encryption can better protect the original information and avoid information theft and exposure.

4.3 Application of Encryption: Cipher Block Chaining
Organizations with important digital information can complicated the process of decryption for illegal people. Thus, a process known as cypher block chaining is applicable. In the process, the plaintext is XORed together with the previous cipher block before the process of encryption takes place. Also, the encryption will be based on a context, therefore, the initial vector and the first block are XORed through a random selection. The encryption steps will rely on the observation that encrypting the ith block is created as a function of each plaintexts in block 0 to the i-1[11].

5. Implementation
The process of implementation uses a simulation table. The simulation uses an initial 12 bit data (n=12) and 4 bits are cut through the encryption doping process (n=4) Using the unrepeated elements the P and D vectors are created in a random process. Furthermore, the Boolean function is used in creating a table with few examples as illustrated below.

| M     | Perm(M)       | Dopt(S)     |
|-------|---------------|-------------|
| 00000000000 | 10101011101 | 100101011100 |
| 00000011000 | 0110111000  | 101101111111 |
| 01011011011 | 111101111111 | 100101111111 |
| 01011011011 | 101010110101 | 101101101101 |
| 01011011000 | 00110001000  | 001101010100 |

The decryption process uses a neural network that is a 3 layer of feedforward network that is important in implementing back propagation algorithm [11]. The content of the decryption process includes 12 neurons in the output, 24 hidden layers, and 16 neurons within the input [11].
Fig. 1. Neural Network Architecture in Decryption Process

Using the neural network toolbox in the MATLAB neural network is implemented. The figure above is a representation of the architecture of the neural network. The process involves initializing the weight matrices with random values between -.5 and .5. The weight matrices used are between the input and the hidden layer and the hidden layer and the output layer. The random value in the table are critical because they are used in initializing the vectors for hidden neuron biases and output neuron biases. The hidden output layer has employed the linear activation function. The iteration is stopped at the instance where the desired output calculated is less than threshold value.

Fig. 2. Original Signal Before Encryption

The figures above are important in evaluation of the mechanisms discussed above. The figures represent the encryption and decryption within the digital and typical signal. The fig. 2 is a representation of the original signal in plain form. Figure 3 shows the signal as illustrated in chain form. Under each sample, the signal is XORed of the original value of the signal.

Fig. 3. XORed Signal
6. Direction of algorithm improvement
The existing encryption algorithms are largely based on the original neural networks with the introduction of hardware, and the encryption algorithm is constructed after analyzing the data information control rules. Although these methods can encrypt the data to a certain extent, the information is generally processed in the storage status and few studies are devoted to encryption during the information transfer process\(^9\). For the latter, signal encryption and deciphering technology can be introduced and combined with neural networks to construct an entire set of encryption algorithms. Through double encryption, the information safety can be more effectively enhanced.

After many years of research in neural networks, the encryption algorithms can be improved by using different neural networks, such as recurrent networks, back propagation networks and fuzzy neural networks. Different encryption methods have been proposed depending on the complexity of information, which facilitates the development of encryption towards intelligence\(^10\). So far, fuzzy neural networks are more frequently used, without special requirements on the application environment. It can be used for abstract processing of information, after which the information is substituted into the network for the encryption.

In some studies, Arnold transformation, homomorphic encryption and CNN system are combined with neural networks. By using the three technologies, the pictures, texts and videos are encrypted, thus raising the complexity of information and difficulty of deciphering as well as boosting the encryption function. The progress made in neural network structure provides a new tool for encryption algorithm studies. The combination of new network system and multiple technologies with introduction of the new information processing technology has enabled the construction of different encryption algorithms.

7. Conclusion
Taken together, as a basic data information processing technology, neural network system has become relatively mature and places a lower requirements on users’ development skills. Thus, the neural network technology has become the preferred choice for developing the encryption algorithms. At present, this technology has found applications in the fields of engineering, user identity recognition, medicine and military. The neural network system can be tailored to users’ safety requirements for encryption, and thus the goal of encryption with the maximum efficiency can be achieved. In future studies on information encryption algorithms, neural networks will continue to occupy an important position as a tool for developing encryption algorithms.

Acknowledgments
Authors wishing to acknowledge assistance or encouragement from colleagues, special work by technical staff or financial support from organizations should do so in an unnumbered Acknowledgments section immediately following the last numbered section of the paper.

References
[1] Norouzi, B., Mirzakuchaki, S. (2017) An image encryption algorithm based on DNA sequence operations and cellular neural network. Multimedia Tools & Applications, 76(11):13681-13701.
[2] Maddodi, G., Awad, A., Awad, D. (2018) A new image encryption algorithm based on heterogeneous chaotic neural network generator and dna encoding. Multimedia Tools & Applications, (3):1-25.
[3] Vino, T., Logashanmugam, E. (2015) Design and Analysis of a High Secure Medical Video Encryption Algorithm with Integrated Watermarking, Compression and Denoising Block. Research Journal of Applied Sciences Engineering & Technology, 11(6):603-609.
[4] Lakshmanan, S., Prakash, M., Lim, C P.(2016) Synchronization of an Inertial Neural Network With Time-Varying Delays and Its Application to Secure Communication. IEEE Transactions on Neural Networks & Learning Systems, 29(1):195-207.
[5] Jang, H., Lee, J. (2018) An Empirical Study on Modeling and Prediction of Bitcoin Prices With Bayesian Neural Networks Based on Blockchain Information. IEEE Access, 6(99):5427-5437.

[6] Thanh, T M., Tanaka, K. (2017) An image zero-watermarking algorithm based on the encryption of visual map feature with watermark information. Multimedia Tools & Applications, 76(11):13455-13471.

[7] Çavuşoğlu, U., Akgül, A., Kaçar, S. (2016) A novel chaos-based encryption algorithm over TCP data packet for secure communication. Security & Communication Networks, 9(11):n/a-n/a.

[8] Wang, K., Wu, J. (2018) High density information encryption and transmission algorithm for large scale database. Journal of Discrete Mathematical Sciences and Cryptography, 21(3):781-787.

[9] Li, C. (2016) Cracking a hierarchical chaotic image encryption algorithm based on permutation. Signal Processing, 118(C):203-210.

[10] Ye, G., Chen, P., Huang, X. (2018) A Chaotic Image Encryption Algorithm Based on Information Entropy. International Journal of Bifurcation & Chaos, 28(1):1850010.

[11] Shihab, K. (2006) A backpropagation neural network for computer network security. Journal of Computer Science, Sep;2(9):710-5.