Information Hiding Technology under the Background of Power System Network Security

Jie Huang1,*, Jing Li1, Jie Wang2, Li Tian2

1 State Grid Hubei Electric Power Co., Ltd, Hubei Wuhan, China, 430077
2 Electric Power Research Institute of State Grid Hubei Electric Power Co., Ltd, Hubei Wuhan, China, 430070

*Corresponding author e-mail: huangjie88@sghel.org

Abstract. Power grid plays an important role in the development of the country and people's life. It can be said that both production and life are inseparable from the power grid. Therefore, when the power system network security threats, the whole life will be adversely affected. Traditional power system network security protection measures have been unable to meet the current demand of power system network security protection. Information hiding technology is an advanced network information hiding technology, which has been widely used in recent years. Therefore, this paper puts forward the research of information hiding technology under the background of power system network security. In this paper, the power system network and information hiding technology are deeply studied. The analysis shows that the latest information hiding technology can play a good role in security protection of power system network, especially for various camouflage attacks. In this paper, according to the actual security requirements of power system network, combined with the main characteristics of information hiding technology, the traditional information hiding algorithm is optimized and improved. In the verification experiment, compared with the traditional algorithm, the NC value of the optimization algorithm in this paper has been significantly improved. The NC value of the traditional algorithm of 5x5 Gaussian low-pass filters is 0.619, while the algorithm of this paper reaches 0.869, the effect is obviously improved. Analysis shows that the algorithm in this paper further improves the NC value of the traditional algorithm, and improves the robustness while ensuring the image quality.

Keywords: Power System Network, Information Hiding Technology, Information Security, Information Transmission

1. Introduction
With the rapid development of power enterprises, there are more and more confidential data in enterprises. With the application of network information technology, data transmission is often threatened. In order to avoid being used by criminals, we need to hide information in the network environment. Because it is more important for the public, it must be hidden [1-3]. But this kind of hidden information needs to change the format of information without affecting the security of information. Data immunity means that the information of host files will be destroyed or lost after multiple processing. The application of data immunity can ensure that the data will not be damaged [4-6].

How to improve the basic operation and management content of information technology has become an important topic for technical researchers. The corresponding technical personnel must investigate the important contents of information technology on the premise of understanding the use function of information technology [7-9]. Combined with the specific use steps, it is necessary to strengthen the basic protection and guarantee, lay the foundation for the follow-up use of information technology, and ensure the basic security of the power grid [10-12].

This paper deeply studies the application of information hiding technology in the power system network in China, and understands that the current power system network in China still adopts the traditional protection technology. Under the background of constantly updating attack technology, the traditional information security protection technology cannot meet the needs of the current power system network protection. Information hiding technology is widely used in network information security, but it is rarely used in power system network at present. Therefore, this paper establishes the research on information hiding technology under the background of power system network security, hoping to strengthen the application of information hiding technology in power system network and further enhance the security protection ability of power system network. In this paper, the traditional information hiding technology is optimized and combined with the latest information hiding technology. In the related comparative experiments, it is further verified that the improved algorithm has better performance than the traditional algorithm, while ensuring the quality; it also greatly improves the robustness of the method. The analysis shows that the research in this paper has achieved ideal results and made a contribution to the research of information hiding technology in the field of power system network security.

2. Power System Network and Information Hiding Technology

2.1. Overview of Information Hiding Technology

Information hiding technology is mainly composed of the following three parts:

(1) Embedding
   The embedded data is embedded into the carrier data by using the hidden key to form secret data.

(2) Transmission
   It mainly refers to the transmission of secret data in the network.

(3) Extraction
   The hidden key is used to recover the embedded data from the secret data.

The purpose of information hiding and information encryption is to protect the storage and transmission of secret information from illegal visitors, but there are significant differences between them. Information encryption uses single key or double key algorithm to convert plaintext into cipher text and send it to the receiver through common channel. Information hiding is different. The secret information is embedded into public information, and then the secret information is transmitted through the public information transmission. The purpose of information hiding is to make illegal visitors do not know who has the secret. However, with the rapid growth of computer computing power, password security is also facing new challenges.

2.2. Role of Information Hiding Technology in Power System Network Security
At present, the power system is gradually upgrading, and the related industries and enterprises have also been better developed. At this time, the internal confidential information of power companies increased significantly. In the current network background, it is very important to protect the corresponding confidential data, avoiding the threat of external factors. In order to achieve this goal, the introduction of information hiding technology has great practical significance, which can better ensure the security of power system related information.

The application and necessity of information hiding technology in network security power system is obvious. With the support of information hiding technology, the reasonable price of electric power transaction is guaranteed, and the copyright of power system software is further protected. Through the application of information hiding technology, we can realize the important protection of key information, such as the transaction price of power companies, and minimize the adverse effects caused by information leakage and failure.

2.3. Information Hiding Model Based on XML

Image and text are the main media of information hiding. Image processing is complex and easy to be damaged after multiple processing. In documents that mainly exist as text, there are free spaces in words and lines. Carefully modify the space from the space, hide some encoded label information to identify the confidential information that needs to be protected. The text in the document does not need any change. At present, the method of hiding confidential information in PDF, HTML and other structured documents has been studied and applied. Extensible markup language (XML), as a language for describing data resources, has strict semantic specification, extensibility and share ability. Based on this function, the interoperability between systems is better, the work of system administrator is more convenient; the convenience of data exchange is enhanced, and can be reused.

2.4. Public Key Encryption Optimization Algorithm

Public key cryptosystems use different encryption and decryption keys. It is a cryptosystem which can deduce the decryption key from the known encryption key, which is not feasible in calculation. The encryption key is public, also known as public key. The decryption key is retained by the user himself, also known as the private key. Messages encrypted with public key can only be decrypted with private key, while messages encrypted with private key can only be decrypted with public key. Anyone who wants to send a message to someone else can be decrypted. At present, the theory is widely used in the fields of confidentiality, signature and authentication. In order to make it better used in the power system network, this paper optimizes and improves the traditional encryption algorithm.

If integer $X$ is used to represent plaintext and integer $Y$ to represent ciphertext, the encryption and decryption algorithm is as follows:

Encryption: $Y = X^e \mod n$ \hspace{1cm} (1)

Decrypt: $X = Y^d \mod n$ \hspace{1cm} (2)

To calculate $n$, the user secretly selects two large prime numbers $p$ and $q$, and calculates:

$$n = p \times q$$ \hspace{1cm} (3)

When $d$ is calculated, the user calculates that the Formula $d$ is satisfied:

$$ed \equiv 1 \mod \phi(n)$$ \hspace{1cm} (4)

Formula (4) is based on the decryption index to obtain the public key and private key.

3. Experimental Methods

Lena image with size of 512x512 is selected as carrier image, and pepper image with size of 64x64 is selected as watermark image. At this time, it is assumed that the watermark is not attacked when it is extracted. The results of this algorithm are compared with those of traditional algorithms.

The specific steps are as follows:

(1) Add noise
In order to detect the robustness of the algorithm to noise, a common noise salt and pepper is added to the watermark image. The noise of salt and pepper with a density of 0.01 was added to the carrier image.

(2) Filtering attack
The median filter with window size of 3x3 is applied to the carrier image to analyze the degradation of image quality and robustness.

(3) JPEG compression
The image is compressed, and the carrier image is compressed when the compression ratio is 40% and 20%. At this time, PSNR value and NC value of the image are detected to compare the image quality.

In order not to affect the image quality, the watermark is embedded into the detail sub image after wavelet decomposition, and the low frequency sub-band with the highest energy is discarded. The watermark embedded in low frequency subband has strong robustness and can be invisible by special processing.

4. Discussion

4.1. Analysis and Comparison of Experimental Results
According to the experimental data, the analysis results in Table 1, Figure 1 and Figure 2 are sorted out. The results show that the improved algorithm is more robust to low-pass distortion when the watermark image quality is the same (PSNR is 41.5 dB after embedding). In the 8-neighborhood average filtering, the NC value of the improved algorithm is about 0.084 higher than that of the original algorithm. The image size is increased by about 0.3 through Gaussian filtering. After the Gaussian low-pass filter with window size of 5x5, the NC value of the watermark extracted before and after the improvement is 0.619 and 0.869 respectively, and the correct watermark can still be extracted. In addition, the robustness of the improved algorithm to JPEG compression is also improved.

The analysis shows that the embedding amount of gray watermark image is larger than that of binary watermark image, so the traditional algorithm is more difficult to achieve better performance. The optimization algorithm in this paper combines the advantages of wavelet decomposition and DCT transform. Experimental results show that the proposed algorithm has a good tradeoff between invisibility and robustness, and can resist various attacks. The improved algorithm embeds the DC and low frequency parts of DCT coefficients into the lowest frequency coefficients of wavelet decomposition of carrier image, which improves the robustness under the premise of invisibility.

Table 1. data table of experimental results.

| Serial number | Test items | Traditional algorithm | Improved algorithm |
|---------------|------------|-----------------------|--------------------|
| A             | PSNR value after watermark | 41.5dB | 41.5dB |
| B             | No watermark NC value | 0.987 | 0.987 |
| C             | 4 domain filtering NC value | 0.909 | 0.947 |
| D             | 8 domain filtering NC value | 0.812 | 0.896 |
| E             | Gaussian filter NC value (3x3) | 0.824 | 0.961 |
| F             | Gaussian filtering NC value (5x5) | 0.619 | 0.869 |
| G             | JPEG compression 40% | 0.927 | 0.991 |
| H             | JPEG compression 20% | 0.893 | 0.973 |
Figure 1. Comparative analysis of filtering results of NC value by two algorithms.
4.2. Analysis of Basic Workflow of Information Hiding

Markup language is more and more widely used in the process of using, and has become a kind of mark that people often use on the network. Therefore, in this process, the XML based distribution process can also be converted to XLS schema. In this process, the element attributes to be processed are targeted. Combining with the specific processing scheme, some element properties need to be reordered. In practice, according to the standardized XML standard, the document form can be modified with some targeted modification process. If the upper and lower documents have a certain procedure change process logically, then in the actual application process, some relationships can also be combined. In order to standardize the development of upper and lower level programs, XML syntax is changed under different application conditions.

4.3. Hidden Information Transmission

Spread spectrum communication is the use of pseudo-random coding system to transmit information data after spread spectrum. The receiver decodes and associates the same encoding to recover the original information data. Using this information hiding technology, SMS can be divided into several parts, and the information transmission can be extended to a wider frequency band in a narrow frequency band. By arranging the transmission frequency sequence in advance, the information can be transmitted to a wider frequency band to achieve the purpose of hiding communication.

(1) Using text files to transfer information

In the process of information transmission, the secret information is encrypted into the selected text, and the camouflage object transmits it to the receiver through the selected transmission route. The receiver uses the corresponding key to extract the secret information, thus realizing the hidden communication.

(2) Using images and digital sound to transmit information

When using image and digital sound to transmit confidential information, the sender encrypts the secret information into the selected noise image and digital sound file to transmit the camouflage object. The receiver extracts the secret information and corresponding key with the receiver through the transmission path to realize secret communication.

5. Conclusions

Whether the power system network is safe or not will directly affect the production of enterprises and the lives of residents, and has an important strategic position in the development of the country. Due to the continuous development of computer technology, the previous means of information attack have been upgraded. The traditional network information protection methods have been unable to meet the protection needs of the current power system network, which has brought a certain threat to the national power security. The research on information hiding technology under the background of power system network security proposed in this paper, through the optimization application of the latest information hiding technology in the power system network, can better make up for the deficiencies in this respect, and has a positive role in improving the security protection system of China's power system network.

References

[1] Nudell, T. R., Nabavi, S., & Chakrabortty, A. (2017). A real-time attack localization algorithm for large power system networks using graph-theoretic techniques. IEEE Transactions on Smart Grid, 6(5), 2551-2559.

[2] Goh, H. H., Chua, Q. S., Lee, S. W., Kok, B. C., & Teo, K. T. K. (2015). Evaluation for voltage stability indices in power system using artificial neural network. Procedia Engineering, 118(8), 1127-1136.
[3] Samson, S., Sundar, R., Ranganathan, T., & Nithiyananthan, K. (2015). Lab view based simple load flow calculator model for three phase power system networks. Birth, 20(2), 148-54.

[4] Li, L., Zhang, X., & Wang, Z. (2015). Fault diagnosis in solar photovoltaic grid-connected power system based on fault tree and brain neural network. Transactions of China Electrotechnical Society, 30(2), 248-254.

[5] Hou, H. (2015). Electric power network fractal and its relationship with power system fault [fraktal mreže električne energije i njegova povezanost s greskom u energetskom sustavu]. Tehnicki Vjesnik Technical Gazette, 22(3), 623-628.

[6] Samson, S., Sundar, R., Ranganathan, T., & Nithiyananthan, K. (2015). Lab view based simple load flow calculator model for three phase power system networks. Birth, 20(2), 148-54.

[7] Houldin, R. (2017). Hiding in plain sight: a note on public goods, information technology, and productivity. Journal of Economic Issues, 51(4), 1158-1161.

[8] Xian, W. L. (2017). Research on the dual digital watermark algorithm based on information hiding technology. Revista de la Facultad de Ingeniería, 32(8), 276-281.

[9] Zhao Zhenzhen, Yang Xiaofei, Huang Jun, & Liu Shupeng. (2017). Image hiding information reconstructing method based on convex optimization. Sensors and Microsystems, 036 (004), 54-56.

[10] Boroujeni, F. Z., & Afshari, D. H. (2018). An efficient rule-hiding method for privacy preserving in transactional databases. Journal of Computing & Information Technology, 25(4), 279-290.

[11] Prabowo, H. E., & Ahmad, T. (2018). Improving prediction error expansion-based data hiding method for securing confidential data. IAENG International Journal of Computer Science, 45(4), 540-551.

[12] Peng, X., & Zeng, G. (2018). An empirical analysis on the diffusion and lagging effects of information technology. Journal of Information Hiding and Multimedia Signal Processing, 9(3), 733-742.