Rsa-Based Digital Image Encryption Algorithm In Wireless Sensor Networks

Gaochang Zhao1, Xiaolin Yang2, Bin Zhou1, Wei Wei3
[1]Xi'an University of Science and Technology,Xi'an 710054,China
[2]Chengdu University of Technology,Chengdu 610059 PR China
[3]Xi'an Jiaotong University, Xi'an 710049, P.R.China
[4]Sichuan University, Chengdu 610065, P.R.China
zhoubxust@gmail.com

Abstract—**Digital Image Encryption is the image processing in the field of a new branch. This paper discusses the modern cryptography, and RSA algorithms. Root According to the data features of digital image itself, designed and implemented digital image based on RSA encryption algorithm, and made further studies of the head. The wireless sensor networks, which self-organized, are data-centered. The current urgent problem with which the wireless faced is how to protect the security of the sensor data effectively. To deal with the weakness of limitation in sensor node resources and the security threats, a novel secure transmission strategy based on information hiding for sensor data security is proposed. In ordering to protect the security of the data, we obtain the sensitive information safely to make use of the advantage of information hiding technique without encryption to safeguard the data security. The simulation experiments illustrate that it is workable to utilize the existing WSN to transmit the sensitive information covertly with the characteristics of lower energy costs and invisibility, and it is suitable for stream data in sensor nodes**.

Keywords-wireless sensor network;secure transmission;data stream;Information hiding Standard. Digital image; RSA; Euler function

I. INTRODUCTION

Wireless sensor network WSN (Wireless Sensor Network) is deployed in the region to monitor a large number of tiny sensor nodes, wireless communication means and form a multi-hop network of self-organizing system [1],[6]-[9]. WSN is widely used in national defense and military, environmental monitoring, traffic management and many other areas of international concern is currently a hot area of research has important scientific value and broad application prospects. WSN is a data-centric network [2],[10]-[12] in many applications, nodes that can sense troops, equipment, materials, terrain and deployment information, locate targets, assess the damage, surveillance and detection of nuclear, biological and chemical attacks, these highly sensitive data once an attacker to obtain, would jeopardize the security of the entire network, it must take effective measures to protect confidential information transmission in WSN security.

This use of information hiding technology using non-encryption to protect data security features, proposes a WSN-based hidden transmission of new data security strategies for resource-constrained sensor node features and face security threats, sensitive information will be embedded into the general information carried out transmission, not only reduces the amount of information transmission, but also to the data collection and security of the secret hidden transmission purposes, to information warfare, especially the network of information warfare provides a new idea

One of modern cryptography, and RSA encryption algorithm

As Internet technology develops, people's privacy and information security technology communications increasing attention. In terms of commercial or military, are widely used modern cryptosystem. Technically, the image information as a data format is fully capable of using modern cryptography for encryption. Modern cryptography can be divided into two categories: one category is the private key cryptosystem, such as DES, IDEA, Blowfish, CAST-256, Mars, etc. [1]. The other is public-key cryptosystem such as RSA, ElGarnal so. These two types of encryption algorithms there is a common feature: they are designed for the encrypted text data in the practical application, the private key password is mainly used for commercial or military encrypt text information, and public key cryptography is often used to encrypt short information, such as the session key and so on. Public-key cryptography largely based on the concept of one-way threshold functions, such as the integer factorization problem, solving the discrete logarithm problems.

Ronal Rivest, Adi Shamir and Len Adleman in 1977, the RSA encryption algorithm proposed by [2] is a public-key cryptosystem is one of the important algorithms. It takes advantage of the field of number theory, a fact that although the two large prime numbers multiplied to generate a composite number is a piece very easy thing, but to a composite number into two prime numbers is very difficult. All factorization problem remains unsolved mathematics a major problem, since there is no efficient decomposition method.

RSA encryption algorithm idea is as follows:

II. KEY PREPARATION

Assumpting x on is that you want to send clear, the current number of electoral heterogeneity of two inter-heterogeneous p and q , let $m = pq$. Take a positive integer e and d , set $ed \equiv 1(\mathrm{mod}\,\varphi(m))$, here, $\varphi(m)$ stand for Euler function , that is $\varphi(m) = (p-1)(q-1)$. This has been used in public key

978-1-4244-6893-5/$26.00 © 2010 IEEE

encryption (e,m) and the private key used to decrypt the (d,m).

Encryption and decryption process can be expressed with the following two formulas.

$$y \equiv x^e (\mathrm{mod}\, m) \quad (1)$$

$$x \equiv y^d (\mathrm{mod}\, m) \quad (2)$$

This algorithm can be applied, because from the public key (e,m), solving the private key (d,m) The process is virtually impossible to implement. Known determined (e,m), That the calculation of the encryption process $y \equiv x^e (\mathrm{mod}\, m)$ the time required is x polynomial function (decryption process is similar); while, if you want to decipher the need for m to do prime factorization (or the complexity of the computing equivalent of this)，To do prime factorization (or the complexity of the computing equivalent of this).

In addition, when compared with the general encryption algorithm, RSA algorithm has obvious advantages of another, without sending and receiving simultaneously on both sides involved in the encryption process.

III. DIGITAL IMAGE ENCRYPTION STATUS

Image in the computer with multi-dimensional arrays in the form of storage, known as digital images (Digital Image). For digital images, encryption algorithm can be divided into two main categories:

An image file as a normal binary data files, using plain password encryption algorithm; 2 images pixel values of pixel address or disrupt the encryption algorithm [3].Arnold transform [4], magic square transform, frequency-based encryption technology and systems based on chaotic image encryption technology [5] are based on the address of the image pixels targeted for replacement operations to achieve the purpose encryption. The difference is that each sequence generated by replacement works differently. The efficiency and security of these algorithms depends on replacement of sequences generated by the efficiency and security.

However, in the encryption process, the efficiency of encryption and security is the unity of opposites. For example: during the encryption process may have a relatively complex algorithm structure to achieve a good encryption effect, but often overlooked encryption process time-consuming, resulting in only a small file, it takes a very long time; some algorithm Encryption time is very short, but it is very simple and very easy to crack.

Although these algorithms can be faster on the image scrambling encryption, but does not take into account the algorithm's security, once the algorithm is open, an attacker can easily recovers the original image based algorithm.

IV. APPLICATION of RSA ENCRYPTION For DIGITAL IMAGES

In summary, RSA encryption algorithm of high security, encryption and decryption phase process on an independent, so they could be used in digital image encryption. However, due to digital image pixel value (gray value or RGB value) of the specificity (0-255), when the results of RSA encryption more than 255, then can only be stored as 255. If the decrypted accordingly, may make a great error. So to use grayscale images (m × n two-dimensional array).

$$image = \begin{bmatrix} \cdots & \cdots & \cdots \\ \cdots & a_{ij} & \cdots \\ \cdots & \cdots & \cdots \end{bmatrix}_{m\times n} \quad (3)$$

For example, with appropriate modifications RSA algorithm is as follows:

1 Initialization grayscale $image$， Integer matrix M， E， the corresponding elements required to meet the RSA encryption algorithm；

2 Encryption：let $image$ pixel x with the public key matrix M， E Corresponding element m， e adopted (1)-equation to be encrypted y， Model 256 to be k and r， to get encrypted digital image $image*$ And the characteristic matrix K；

3 Decryption：let $image*$ the pixel value r and characteristic matrix K The corresponding element in the formula by the combination of $y = 256k + r$, get y， with the public key matrix M，The private key matrix D the corresponding element in m， d By (2)-equation to decrypt and thus obtain the original gray image $image$。

Color RGB image is the m×n×3 three-dimensional array of:

$$image = \begin{bmatrix} \cdots & \cdots & \cdots \\ \cdots & (r_{ij}, g_{ij}, b_{ij}) & \cdots \\ \cdots & \cdots & \cdots \end{bmatrix}_{m\times n} \quad (4)$$

The first encryption algorithm mentioned above, among the various operations are aimed at two-dimensional array, and it is impossible to achieve the right color image encryption. Therefore, an array of two-dimensional image of first:

$$image' = \left[image_r, image_g, image_b \right]_{m\times 3n}$$

$$image_k = \begin{bmatrix} \cdots & \cdots & \cdots \\ \cdots & p_{ij} & \cdots \\ \cdots & \cdots & \cdots \end{bmatrix}_{m\times n}, k = r, g, b$$

（5）

image' has been transformed into two-dimensional array, can be RSA encryption and decryption, the process is with the operation of exactly the same gray-scale image.

In the P4 1.5G computer using Matlab mathematical software program to achieve the above encryption algorithm, and 128 × 128 × 8 B of the Lena gray image in computer simulation (Figure 1 --- Figure 3), encryption time of 331ms, decryption time for 495ms, this method is more rapid. Pairs of 256 × 256 × 8 B of the color images in computer simulation (Figure 4 --- Figure 6), encryption time and decryption time is about the original 10 times slower.

Fig.1 pre-gray image encryption

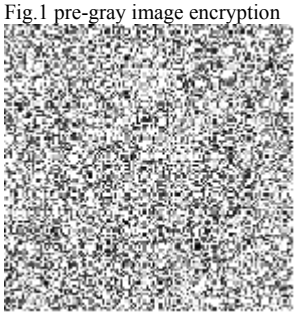

Fig.2encrypted gray image

Fig.3 gray-scale image after decryption

Fig.4 Encrypted pre-color image

Fig.5 Encrypted color image

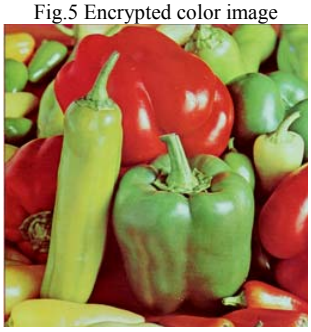

Fig.6 After the color image decryption

V. CONCLUSION

In this paper, based on RSA encryption algorithm, combining features of digital image itself, designed and implemented digital image based on RSA encryption algorithm, high security, can grayscale images faster encryption. When less demanding in terms of time-consuming, but also for encryption of color RGB images. The next step will combine a number of other common image encryption algorithm more in-depth study.

Sensor network is data-centric network, this paper presents a sensor-based information hiding transfer mode network security, data security for WSN has opened up a new research approach, the main contribution is:

(1) the use of information hiding technology will be hidden sensitive data secure transmission, can reduce the sensor nodes process the data that is being monitored, the risk of interception, while traffic is greatly reduced;

(2) designed for streaming data in real-time information hiding algorithms can be efficient, low energy consumption to achieve the hidden and extract sensitive information.

Experiments show that a good security program to realize the security of sensitive information collection and transmission, improve the safety performance of WSN; the

same time, the reduction of traffic to reduce network energy consumption and prolong the life cycle and, accordingly may obtain more information.

In the WSN security mechanisms, the sensor nodes to minimize resource consumption and security are a pair of hard to balance the maximization of contradictions. Therefore, the model need to design efficient and safe, high-capacity embedded algorithms, encoding resistance to the attack, safer, more efficient security mechanisms have yet to be further studied.

ACKNOWLEDGMENTS

We would like to thank the anonymous reviewers for their valuable comments.

REFERENCES

[1] Bruce Schneier. Applied Cryptography -Protocols, algorithms, and source code in C[M].Second edition. New York: John Wiley &Sons, 1996.

[2] Fan Yun, LIU Hong-wei. Group with combined coding [M]. Wuhan: Wuhan University Press, 2002.

[3] Xingsha Liu, Li Min, FEI Yao-ping. A high-security digital image encryption algorithm [J]. Microelectronics and Computer, 2007,24 (2) :21-23, 27.

[4] Chonggang Wang, Bin Li, Y Thomas Hou, et al. A RobustActive Queue Management Scheme Based on Packet LossRatio [C]. IEEE INFOCOM2004, 2004: 1~12.

[5] Yi Kai-xiang, SUN Xin, SHI Jiao-ying. A kind of image sequences based on chaotic encryption algorithm [J]. Computer-Aided Design & Computer Graphics, 2000,12 (9) :672-676.

[6] K.P. AlSakib, T.D. Tran, S.H. Chong. A Key Management Scheme with Encoding and Improved Security for Wireless Sensor Networks. ICDCIT 2006:102-115.

[7] H.W. Chan, A. Perrig. PIKE: peer intermediaries for key establishment in sensor networks. Proceedings of the IEEE INFOCOM 2005. Piseataway, USA, March 2005:524-535.

[8] A. Perrig, Szewczyk R, Wen V, et a1. SPINS : Security Protocols for Sensor Networks. Wireless Networks, 2002. 8(5): 521-534.

[9] L. Esehenauer, V. D. Gligor. A key-management scheme for distributed sensor networks. Proceedings of the 9th ACM Conference on Computer and Communication Security. USA: ACM. 2002:41-47.

[10] Chan H, Perrig A, Song D. Random key predistribution schemes for sensor networks. Proceedings of the IEEE Computer Society Symposium on Security and Privacy. Piscataway, USA, 2003:197-213.

[11] W. Du, J Deng, et a1. A pairwise key predistribution scheme for wireless sensor networks. Proceedings of the l0th ACM Conference on Computer and Communications Security. USA, ACM, 2003:42-51.

[12] D. Liu, P. Ning. Location-based pairwise key establishments for static sensor networks. Proceedings of the 1st ACM Workshop on Security of Ad Hoe and Security of Ad Hoe and Sensor Networks. USA, ACM, 2003:72-82.