様式第２号（第５条，第１１条関係）

「課程博士用」

学 位 論 文 の 要 旨

専　　攻	安全システム工学　専攻	ふりがな 氏　　名	ヤン ホウ Yang　Peng
学位論文題目	Research on Signal Processing for a Virtual Optical Encryption System （仮想光暗号化システムの信号処理に関する研究）		

学位論文要旨

In recently rapid development of computers and information technology, the digital information on the public networks is often unable to resist unauthorized attacks. To make a system more secure, a robust encryption algorithm should be designed an encryption system that encryption keys are unique and unpredictable. Some existent systems are using long-size encryption key, however, a long size encryption key will create another problem which is the speed and the efficiency of the encryption process. It means that increasing security of a message will scarify in the processing speed. The optical encryption technology based on holographic is relying on a new technology that has many advantages such as high speed, multi-dimensional and high capacity.

This research's work presents a new method for encrypting holographic information based on optical and acoustic signals called a Virtual Optical Holographic Encryption (VOHE) system for underwater communications that can be applicable for communications between deep submergence research vehicles. The optical encryption system provides essential parameters for constructing secure communications such as the propagation wavelength (λ) and focal length (f) of the Fourier lens, which are considered as keys for implementing encryption and decryption processes. The transmission's media such as optical signals and acoustic signals are implemented as means for sending interference fringe pattern (IFP) that carries object information to a receiver. The optical signal is used to encrypt the object information, and the encrypted signal is carried by an acoustic signal, and then the signal will be transmitted to the acoustic channel for a long-distance transmission.

The VOHE system employs virtual optical encryption system was simulated based on COMSOL Multiphysics simulation software. The encrypted signal of precedent VOHE systems was based on a symmetric key encryption method. In this method, two users such as a sender and a receiver select a VOHE system's key (λ, f) in advance then they use the VOHE system's key to communicate a system's cipher (IFP) over a public channel. Occasionally, users can exchange system's keys periodically. However, the VOHE system may lose system's keys during keys exchange processes. To solve this problem and to strengthen the security over VOHE, hybrid algorithms of Diffie-Hellman (DH) and RSA are introduced.

Both RSA and the DH algorithms are recently used as the foundation for the security we use today. However, these technologies are limited for reinforcing security for data transmission. In this research's project, we introduce two encryption systems, the first one is based on RSA algorithm called an expanded RSA (ERSA) algorithm, and the second one is based on an expanded Diffie-Hellman (EDH) algorithm. Both systems are using complex functions for sending crucial data such as system's key (λ, f) for ERSA algorithm and encrypted holographic information (IFP) for EDH algorithm, respectively.

To evaluate the security and efficiency of the proposed ERSA algorithm and EDH-C algorithm, an expanded Pollard's Rho method was applied and the obtained results have been investigated.

In the VOHE system, the ERSA algorithm for encrypting system's key (λ, f) and the EDH-C algorithm for encrypting system information (IFP), respectively, are more appropriate methods for strengthening the security of the data transmissions.

To determine accuracy of the information retrieved by the proposed technique, the minimum mean square error (MMSE) was conducted to evaluate the accuracy of the received signal. Numerous results of comparison between the EDH algorithm and the traditional DH algorithm have been acquired. From the results of MMSE, we have perceived higher MMSE for traditional DH than EDH algorithm. We concluded that the EDH method has the highest performance than DH method in view of MMSE.

Finally, the National Institute of Standards and Technology (NIST) method is applied to evaluate the security of proposed ERSA and EDH-C algorithms in view of randomness, unpredictability and complexity of the transmitted message over an insecure channel. The results have showed that both ERSA and EDH-C are capable to provide highest security than RSA and conventional DH, respectively.

In our future research, we will broaden our investigation by comparing EDH-C algorithm and ERSA algorithm with other various hyper-complex number systems. We considered in this paper that the encryption process was done between only two nodes. In future research, we will further investigate the security of data transmissions over multi-node network systems.

注）和文 2,000 字以内又は英文 800 語以内　　続紙　有□　無■