Study on Encryption Techniques of Distance Measurement in Laser Fuze

Lei Yiyan\textsuperscript{1a} Yi Kang\textsuperscript{2b} Zhao Yuting\textsuperscript{3c}

\textsuperscript{1}Institute of Information and Communication, National University of Defense Technology
Guangming Road 5th, Wangqu Street, ,
Changan, Xi’an, Shaanxi, China
+86 13347411716

\textsuperscript{2}Institute of Information and Communication, National University of Defense Technology
Guangming Road 5th, Wangqu Street, ,
Changan, Xi’an, Shaanxi, China
+86 13347411716

\textsuperscript{3}Institute of Information and Communication, National University of Defense Technology
Guangming Road 5th, Wangqu Street, ,
Changan, Xi’an, Shaanxi, China
+86 13347411716

\textsuperscript{a}75366837@qq.com \textsuperscript{b}penfangs@163.com \textsuperscript{c}xty_zyt@163.com

ABSTRACT: To improve the anti-interference performance of laser fuze, the polarized properties of laser in the laser fuze is used. By controlling the polarized properties of laser, the target and get the information of distance can be recognized. According to the polarized properties of scattering light, the laser fuze distinguishes the target from the background, which can weaken the influence of the background light and active interference. At the same time, some key technologies of laser fuze, such as rotation of bomb and information encryption and so on, are also studied.

CCS Concepts
\begin{itemize}
  \item CCS $\rightarrow$ Computing methodologies $\rightarrow$ Modeling and simulation $\rightarrow$ Model development and analysis $\rightarrow$ Modeling methodologies
\end{itemize}

1. INTRODUCTION
With good characteristics of sharp directionality, monochromaticity, coherence and high light, laser is widely used in the weapon system. Laser-fuse is one of them. According to relevant data and information, 80%-90% of the air-to-air missiles were equipped with laser-fuse, and almost all the fuses on the antitank missiles are laser-fuse in the world. What’s more, the well developed laser guided threats also stimulate the development of the laser countermeasure technology. Laser jamming devices can effectively jam laser threats including laser range finder and laser guided weapon, which can help to protect the safety of our own platform. Laser active jamming technology includes laser ranging distance deception
jamming technology, laser guided weapon active jamming technology, laser proximity fuse active jamming technology, laser blinding weapons and high energy laser weapons, etc. Active jamming problems need to be solved if we want the laser fuse to work better in the war. It’s very important for us to find out how to counter active jamming from the enemy effectively and improve the performance of laser proximity fuse. In this thesis, the encryption of the range finding information sent by laser fuse is studied first, and an encryption scheme that combining chaos sequence with polarization control is proposed to enhance the anti-jamming capacity, especially anti active jamming capacity of the fuse.

2. PRINCIPLE OF LASER FUSE RANGING

The Laser fuse is developed on the basis of laser ranging technology. Normally, the pulse ranging technology would be used. One light pulse or a bunch of light pulse would be sent to the target through a paused laser, and the time the light pulse use to get the target and return to the receiver would be recorded, so that the distance between the paused laser and the target can be calculated.

Given R is the range of the target, t is the time that light pulse need to travel to and return from the target, and c is the propagation velocity of light in the air, then

\[ R = \frac{ct}{2} \]

(1)

If pulse laser ranger is used, t will be timed through counting the number of clock frequency pulse that the counter received. During which period, if n clock frequency pulse are received by the counter, the time interval between each clock frequency pulses T, then the oscillation frequency of clock frequency pulse is \( f = \frac{1}{\tau} \), and

\[ R = \frac{cn\tau}{2} = \frac{cn}{2f} = l \cdot n \]

(2)

In which, \( l = \frac{c}{2f} \) represents the range increment, with n clock frequency pulse, then the range R can be got.

3. THE ENCRYPTION OF RANGING INFORMATION

To improve the anti active jamming capacity of laser proximity fuse, the polarization state of the laser beam is controlled after encrypting the chaos sequences, which will help to keep the information privacy. Polarization status will be modified at set intervals (e.g. 0.1 second) according to the changes of the chaos sequences. Only after receiving reflected beam that is correspondence with the laser beam which is sent for many times in a row, do we confirm the returned signal, electrical signals will be generated and feed to the firing circuit, which, to a large extent, can avoid active jamming.

3.1 Encrypting Ranger Information with Chaos Sequences

To generate chaos sequences and reduce complexity of the system, single dimensional Logistic was chosen to generate chaos sequences. Mapping relations of the logistic map is:

\[ x_{i+1} = \lambda x_i (1 - x_i), \quad x_i \in [0,1], \lambda \in [0,4] \]

(3)

Through this, a set of chaos sequences can be taken as the key stream \( M_n (m) \) to modulate ranging information \( S_n (m) \) with different computing methods including addition, subtraction, multiplication and division, and then the encrypted ranging information is got. And decryption is to use the key stream on encrypted information with inverse computing methods, and then the decrypted ranging information \( C_n (m) \) can be got. If the beginning and the end of the original sequence is left off, or the date is processed with other ways including splitting, shifting or some kind of combination, and encrypt the information with random sequence as the key stream, the anti-decipher ability will be enhanced. Here take the Logistic map when \( \lambda = 4 \) as an example, with processed data as key stream \( K_n (m) \), the ranger information can be modulated. The encryption process is:

\[ E_n (m) = S_n (m) \oplus K_n (m) \]

(4)

And the decryption process is:
In the equations, $K_n(m)$ and $K'_n(m)$ are encryption key stream and decryption key stream respectively, and $E_n(m)$ and $C_n(m)$ are encrypted ranger information and decrypted ranger information. In the (4) and (5) equations, if $K_n(m) = K'_n(m)$, $C_n(m) = S_n(m)$.

$$C_n(m) = E_n(m) \oplus K'_n(m)$$

### 3.2 Encrypt with the Laser’s Polarization Character

After illuminating the target with laser beam with polarized laser beam, the echo signals reflected from the target, jamming signals from the enemies and echo signals reflected from the background are received. The surface of common man-made objects like airplanes, tanks are approximately smooth, while the background is normally with rough surface, which might cause greater polarization than man-made smooth objects. As a result, the objects can be separated from the background, and the influence of echo signals to the fuse system can be reduced. In addition, with the polarization of echo signals, the active jamming signals can be separated from the enemies and the useful echo signals.

![Fig 1. Working principle of the launching system with polarized laser fuse](image1)

Fig 1 is the working principle of the launching system with polarized laser fuse. Through beam splitter $F$, the laser beam is divided into two same laser beams, which separately passed two polarizes with vertical vibration direction $P_1$ and $P_2$. And the two beams will be linearly polarized lights with orthogonal polarization direction. After encrypting the ranging information, the two linear polarized light beams can be controlled to control the variable optical attenuator (VOA). In accordance with the vector composition principle, if the beam light sent by emitter is elliptically polarized light composed with two linearly polarized lights with orthogonal polarization direction, the polarization state of the light beam can be controlled by variable optical attenuator (VOA). And after combined by the combiner, elliptically polarized light will be sent through optical antenna.

![Fig 2. Working principle of the receiving optical system](image2)

While Chart 2 shows the working principle of the receiving optical system. After passing through two orthogonal analyzers, the two light signals reflected from the target will be detected by an optical detector for their light intensity, $I_x$ and $I_y$ respectively. Through calculating the angle of polarization of the received elliptically polarized lights, we can know whether it is the reflected light from the target. In the equation,

$$[\alpha] = \tan^{-1} \frac{I_y}{I_x}$$

$\alpha$ is the polarizing angle. Light intensity of vertically polarized light and horizontally polarized light can be detected by a photo electronic detector. $[.]$ means we only get round numbers, which might reduce the influences of atmospheric transmission and computational accuracy on the accuracy of the signal demodulation. Then, in the receiving optical system, only by demodulating and sending the returned signals that enjoy the same polarization state from the sending end, can we realize the purpose of ranging, target exploring and secrecy keeping.
4. CONFIDENTIALITY ANALYSIS OF THE EFFECTS OF INFORMATION ENCRYPTION

4.1 Theoretical Analysis
The first of all, the ranging information with chaos sequence is encrypted, which helps to increase the secrecy of ranging information. Chaos is a random process that generated from nonlinear system. Chaos signals are generated from deterministic equation, but its motion trail is highly sensitive to the initial conditions. Even a minute change might cause the trajectory is exponentially separated. What’s more, the sequence can be infinitely long; the configuration is a lot like random noise; auto-correlation function is like ballistic and cross correlation function approximates zero, and the power spectrum almost cover all the frequency range. All of these characters make chaos sequences suitable for sequence encryption.

Secondly, the polarization is used into the fuse, and the polarization of laser beam with ranging information is controlled. Then in the receiving optical system, only by demodulating the signals that share the same polarization state with the laser beam we send, can we reduce the interference of bias light and active jamming, and increase the secrecy of the system.

4.2 Computer Simulation
We take $x_0=0.100100$ as the initial value of the Logistic map, generate a chaos sequence, cut out a piece of chaos sequence when $N = 1000$ as encryption sequence to encrypt the ranging information. Encrypted ranging information is used to control the polarization state of the laser beam and polarization state is modified in accordance with the change of encryption sequence.

Fig 3. Simulation diagram of the receiver receiving reflected signals

Fig 4. Simulation diagram of the receiver receiving background reflected signals and jamming signals

Fig 3 is the simulation diagram of the receiver receiving reflected signals; while fig 4 is the simulation diagram of the receiver receiving background reflected signals and jamming signals. From these two charts, we can see that with controlling the polarization state of laser beam through encrypting
ranging information with chaos sequences, we realized the purpose of ranging information. And it can help to enhance the secrecy and anti-active jamming capacity.

5. CONCLUSION
In this thesis, the encryption of the range finding information sent by laser fuse is studied first, and an encryption scheme that combining chaos sequence with polarization control is proposed, to enhance the anti-jamming capacity of the fuse. Computer simulation proves that the confidentiality and anti-jamming capacity of this encryption scheme is good.

ACKNOWLEDGMENTS
Our thanks to ACM SIGCHI for allowing us to modify templates they had developed.

REFERENCES
[1] Wang De. Laser Fuzes and Their Development Situation [J]. Journal of Changchun Institute of optics and Fire Mechanics, 2001, 24(1): 62-66
[2] Liang Zhu. Course of optical principle [M]. Bei Jing: Beijing University of Aeronautics and Astronautics Press, 2005
[3] M.Born, E. WolfPrinciples of Optics [M]. Bei Jing: Science Press, 1985
[4] LI Quan, LIU Ze-jin, SHU Bo-hong, LU Qi-sheng, CHEN Qian-rong. Application of polarization diversity in active imaging [J]. High Power Laser and Particle Beams, 2005(3): 32-36
[5] WANG Ning, LI Guo-hua. ADJUSTMENT OF LEFT-HAND ROTATION OR RIGHT-HAND ROTATION WITH λ/4 WAVEPLATE[J]. Journal of Applied Optics, 2001, 22(2): 32-34
[6] Zhou Mu-chun, Chen Yan-ru, Zhao Qi, Yuan Xing-qi, Wang Yun. Study On Dynamic Detection of Polarization States in Laser Guidance[J]. Chinese Journal of Scientific Instrument, 2005, 26(8): 87-89
[7] Wu Jian-zhen, Xie Jian-ying. A Review on Chaotic Secure Communication[J]. Communication Technology, 2003, 135(3): 87-89