Security System for Surveillance Radar Network Communication Using Chaos Algorithm

Nova Hadi Lestriandoko
Research Center for Informatics
Indonesian Institute of Sciences (LIPI)
ryan@informatika.lipi.go.id

Tutun Juhana
School of Electrical Engineering and Informatics
Institut Teknologi Bandung (ITB)
tutun@stei.itb.ac.id

Rinaldi Munir
School of Electrical Engineering and Informatics
Institut Teknologi Bandung (ITB)
rinaldi-m@stei.itb.ac.id

***Abstract*—Surveillance radar network is the network of some radar station to monitor and keep watch ship/vessel traffic. The communication of these station used tcp/ip over internet and local area network. The security system is an important part that can not be ignored for network communication. This paper proposed a prototype of security system for surveillance radar network, which is handling the security of communications over the Internet between a radar station to master station. The system is designed to protect the radar data against unauthorized parties. From the previous work, there was a weakness in the pseudorandom number generator. The generated number could not satisfy the randomness, it might be raise a security problem. Thus, Pseudorandom Number Generator (PNRG) using chaos algorithm was added to strengthen the salt cryptographic scheme. The analysis of result will be discussed to obtain the advantages of new system. Finally, a layered security system has been developed by taking advantage of a variety of encryption algorithms to get the best protection for the security of surveillance radar network communication.**

Keywords—chaos algorithm; security system; surveillance radar network; salt cryptography; Identity Based Security(IBE)

I. INTRODUCTION

Radar ISRA (Indonesian Surveillance Radar), the first FWCW maritime radar (Frequency Modulated Continuous Wave) was made in Indonesia, is used to detect and measure the distance of a ship at sea with a low transmit power and does not cause a large radiation. [1] [2]. Radar system consists two main parts: transmitter and receiver [3]. The results of detection are shown on Radar display unit, where this unit processes the received signals into information that can be interpreted easily by the users. Antenna control has a function of synchronizing the antenna movement with the scanning movement on the Display unit. Synchronizer adjusts the transmitted signals with the required display of objects. In the integrated radar networks used to monitor the movement of ships, there are a lot of radars, each connected to the main station through the Internet (TCP / IP). The figure 1 presents the illustration of the radar network in Indonesia for sea surveillance. One of the advantages of this network radar is a radar can be controlled from a distance / from anywhere as long as it is connected to the Internet network. It can also pressure the communication cost. On the other hand, the vulnerable security problems arise when using the internet. This is what underlies the need for a security system to prevent the assault, theft, and illegal data modification.

There are some technologies that can be used to secure the internet communication: cryptographic system, firewall, Intrusion Detection System (IDS), Anti-malware software and scanner, Internet Protocol Security (IPSec), and Secure Socket Layer (SSL) [4]. In this case, the radar security focuses on the using of cryptographic system for preventing data communication attacks. There are several services in data security that have been classified into several types: confidentiality, authentication, integrity, non repudiation, access control, and availability. In this case, the surveillance radar network communication only focuses on confidentiality, authentication, and integrity. Confidentiality ensures that information in a computer system and sent the information can only be accessed for read by the authorities. Authentication ensures that the authenticity of a message or electronic document is correctly identified, with the assurance that the identity is not false. Integrity ensures that only authorized parties can modify computer system assets and information.

The concept of a secure communication on the Internet is the use of cryptography. Overall, there are two categories of cryptographic systems: symmetric key encryption and public key encryption. In symmetric key (also called the conventional cipher), the sender and receiver use the same secret key for encryption and decryption of messages. Many encryption algorithms have been created and used, for examples are DES, AES, RC5, blowfish and IDEA. When the input data is very long, the symmetric key algorithm will divide the data into equal-sized data blocks (except for the last block) and do the encryption / decryption of the data block by using the same algorithm and key. In public key encryption, public and private key pair will be generated simultaneously. One of the two keys to be used for encryption, while the other for decryption. Examples of well-known public-key encryption are RSA, Public Key Infrastructure (PKI), Quantum Public Key cryptosystem and Elliptic Curve Cryptography.

Digital signature is a method to add a unique sign into a digital file, either text or image, which is used to authenticate digital files. Digital signatures are designed to make the writers and content validation more efficient. When a document is digitally signed, it will remain in its original form so that everyone will be able to read it. Popular algorithm used for digital signatures are hash functions MD5 and SHA-1.

Basically, the strength of an encryption is in the key length and in the algorithm [5], which is based on the latest recommendation, 128 bit is enough to protect the data for 28 years (level 7 long-term protection by ECRYPT II from 2012

978-1-4799-7447-4/14/$31.00

to 2040) [6]. Pseudo random number generator (PRNG) is a way to increase the strength of the encryption algorithm using random key generation. Yarrow and Fortune algorithms developed by Bruce Schneier and Niels Ferguson [7] are examples of this PRNG. Development of other PRNG published by M.Shafeeq et al [8] discusses some of the problems in cryptography and introduces a new method of random key encryption (RKE). The other random number encyption development is encryption based on random sequence generation using iteration matrix and quadruple vector introduced by A.Chandra Sekhar et al [9]. On the other side, the publication of K.Marton et al [10] analyse the importance of randomness in a digital cryptography to cover weaknesses in some cryptographic algorithms. Randomness is an important thing to secure the data that be unknown, unguessable, unpredictable, and unrepeatable. Salt Cryptographic is a way to satisfy the fourth element. Salt Cryptography is a method of adding bits or bytes or characters in a message before it is encrypted. There are two types of salt cryptographic, the constant salt and the random salt. This method is very useful to prevent attacks on cryptography, because the encrypted radar data may still be retrieved using network traffic analysis to be decoded.

R.Munir et al, in their papers [11][12], used the chaos algorithm to generate the pseudorandom number. It can be used to various application, for example information hiding, pseudorandom number generator, watermarking, encryption, key generator and else. The chaos algorithm can produce random number even though the system is deterministic. The values of the resulting chaos would be in the range between 0 and 1.

The paper is organized as follows: Introduction to Chaos theory in Section 2; the proposed security system with chaos algorithm to strengthen the salt scheme in Section 3; experimental results and analysis are performed in Section 4; finally, some conclusions are drawn in Section 5.

II. Introduction To Chaos Theory

A. Chaos Theory

Chaos theory is derived from the theory of systems that show irregular occurrence, despite the fact that this theory is used to explain the occurrence of random data. Inventor of chaos theory is a meteorologist, Edward Lorentz, in 1960 when he made a model of weather forecasts. The mathematical model is calculated repeatedly to obtain weather forecasts weather in the future. The longer time weather forecasts are calculated, the length of iterations to be performed. By changing just a few iterations of the initial value 0.000127, he discovered that the weather forecasts are produced having a large divergence. Figure 2 shows a plot of the curve of iterations on the weather models using different curve initial values of 0.000127. This phenomenon is called as the wings of a butterfly effect (butterfly effect), which states that small differences in the initial iteration values of the two curves can be compared with the flapping wings of a butterfly:

> The flapping of a single butterfly's wing today produces a tiny change in the state of the atmosphere. Over a period of time, what the atmosphere actually does diverges from what it would have done. So, in a month's time, a tornado that would have devastated the Indonesian coast doesn't happen. Or maybe one that wasn't going to happen, does. (Ian Stewart, Does God Play Dice? The Mathematics of Chaos, pg. 141)

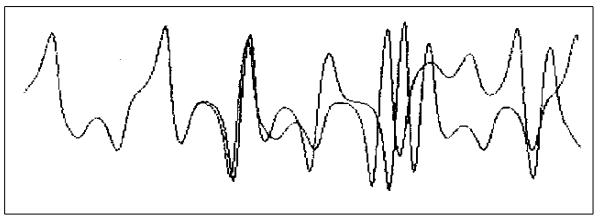

Fig. 1. Lorenz's experiment: the difference between the starting values of these curves is only .000127. (Ian Stewart, Does God Play Dice? The Mathematics of Chaos, pg. 141)

This phenomenon, the sensitivity to changes in the initial value, is common in the chaos theory which is also known as sensitive dependence on initial condition. This sensitivity means that small differences in the initial value of the function, such as a change of 10-100, after the function is repeated several times, will result in a huge difference in the value. For example, if the equation of chaos begins with the initial value of 32, and at other times 32.000001, then after 100 iterations the value equation with the initial value of the first may be 137.54, while the value of the second may be 1160,934 [15]. One of the simplest chaos functions are logistic equation in the ecology that is used to simulate the growth of populations of species:

$$f(x) = r\,x(1-x) \tag{1}$$

$$x_{i+1} = r\,x_i(1-x_i) \tag{2}$$

In the equation (1) and (2) above x is the population of the species at time intervals determined by x_0 is the initial value of iteration. Area of origin x is from 0 to 1, which in this case 1 states the maximum population and 0 states extinction, while 0 < r <4 constants r denote the rate of growth. When 0 < r <1, regardless of the initial value will result in extinction (ie the value of x at the end of the iteration is 0). If 1 < r <3, the function converges to a value (fixed-point), the value of r which produces the system has a period of one cycle. For example, if r = 1.5 and x_0 = 0.25, then the equation iteration will converge to a fixed-point value of 1/3 (or 0.3333 ...). When r = 3, the curve is split into two functions (termed the bifurcation) produces two distinct populations values, which means the value of x periodically oscillate from high status to low status. The period of the system at this r value is two. When r increases again, the function curves split again into four, which means that the values of x the resulting oscillating between 4 value. The period of the system at this r value is four. Thus beyond the bifurcation becomes faster again into 4, 8, and 32 with the increasing value of r to arrive at a certain value of r also appear chaotic nature. At this point it is not possible to predict the behavior of the system. We can see that when r > 3.75 the system began moving rapidly towards the area of chaos[13]. Finally, when r = 4, the iteration depends entirely on the initial value x0 and the resulting values appear random even though the system is deterministic [14]. The

values of the resulting chaos would be in the range completely between 0 and 1 [15].

B. *Cropping Function*

Cryptographic operations in the set of integers whose value is from 0 to 255, while the value of chaotic sequence is used as the key stream is a real number between 0 and 1 To row values can be used chaotic encryption and decryption, then the value is converted to an integer value chaos. There are several techniques that can be used conversions, common techniques such as taking the last 3 digits in the part of the real numbers. For example, 0.024568 taken from the last 3 digits of the part is 568.

C. *Random Number Generator Using Chaos Algorithm*

Chaos generated values of equation (1) by taking the constant r = 4.0. Normally, the value of xi is computed directly from the chaos previous value, x_{i-1} This means that if someone knows a value x_i of sequence values chaos, then he can use to generate x_i, x_{i+1}, x_{i+2}, ..., x_n which is then used to decrypt ciphertext.

To add strength to the system, then the value of x_i raised after a certain number of iterations. The goal is to eliminate the correlation between the values of chaos. The number of iterations required to compute the value of the first chaos, x_1, is determined by the initial value, x_0. The initial value is converted to an integer by cropping function, the result is the number of iterations required to iterate equation (1). X values obtained at the end of the iteration act as "x_0" new to calculate x_1. For x_2, x_3, and so on, the number of iteration is determined from the number of iterations for the value of the previous chaos coupled with size.

In this way, a person who knows a certain value xi may not be able to calculate x_{i+1} without knowing the number of iterations needed to iterate equation (1). The number of initial iterations is determined by x_0. Thus, the initial value is the value that will determine the security of stream ciphers. There are infinite number of values between 0 and 1, therefore exhaustive key search to find x_0 be something that is not possible is passed. Moreover, as already described chaos functions are sensitive to small changes in the initial value, so that if the initial value of the opposing party tried very close to the value that is used to encrypt the data, the opponent will still obtain the output is wrong.

III. PROPOSED METHOD

ISRA radar network consists of two surveillance radar stations and one that mounted on a truck (mobile radar). Each radar station consists of several modules, the antenna Tx / Rx, Analog to Digital Converter (ADC), radar signal processing (FFT), motorcycle radar, radar display, and object radar extraction. Radar network communication (from radar station to monitoring station or master station) is done via TCP / IP through the internet as shown in Figure 2.

In the each radar station was installed a modem for sending data to a web server. Master station calls a web-based application that displays data from each radars into an integrated map, which can be used to monitor sea traffic. The location of the radars are in Anyer Beach - Banten, Pantai Kelapa Dua-Merak, and Lampung.

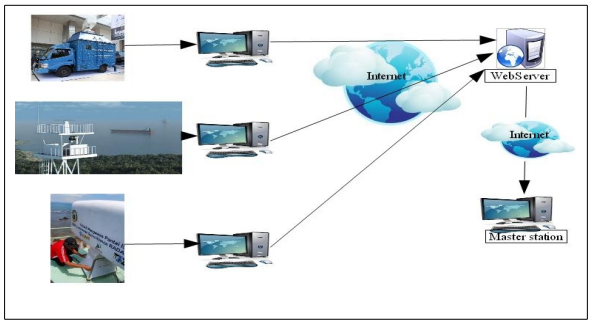

Fig. 2. Radar Network Communication[16]

A. *The Security Design*

The research in this paper focuses on the security radar data communication via the internet. That is the transmission data from object radar extraction module to the web server. If there is no security system, the data flow delivery can be extracted directly from the module to the web server. If a security system is added to a radar system between the extraction module and a web server, then there are some difficulties that arise, the differences in language between the sender and the receiver causes the encryption and decryption processes be undone. The solution of this problem is to create an intermediate medium that can communicate with both sides, that is the localhost. In the localhost, the encryption and salt will be done. Next, the encrypted radar data is sent to the web server. The process of reading (decryption process) is done on the web server. Further, radar data is stored into the database. Monitoring station / master station only display and retrieve data that has been saved in the database server. This security scheme can be seen in the following figure 3.

In the each module, there are main functions that are used to data transmission and data encryption. The functions of each module are shown in Figure 4. Those are data transmission function, receiving data, encryption and salt, and the used protocol. Display module sends data using winsock with TCP / IP to a module extraction. Extraction module sends the clustering results using httpPost, a protocol used for transmitting data securely on web programming (for a username and password), to localhost. From here, encryption and salt is done first before being sent again to the webserver. After the data was received in the webserver, it was decrypted and saved into database server. Shortly before saving, the data is verified to guarantee the originality.

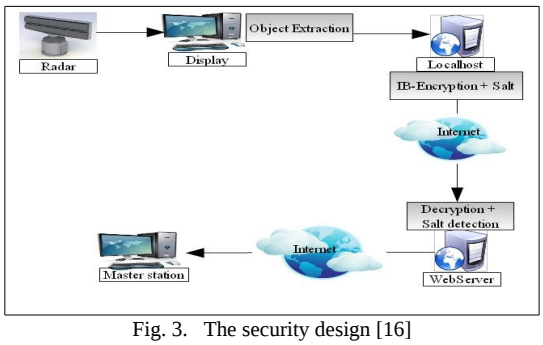

Fig. 3. The security design [16]

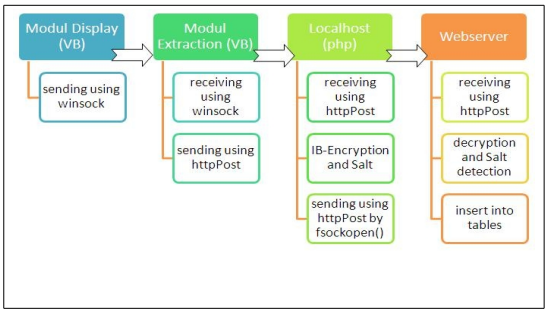

Fig. 4. Data transmission[16]

B. *Salt Cryptographic with Chaos Pseudorandom Number Generator*

Salt cryptography is additional random bits into cryptography, commonly used in one-way cryptographic. Input can be a character or a word or phrase, which is encrypted with a password. Salt can also be combined with a password using the derivative function (key derivation function) to generate the key used by the encryption algorithm. Cryptography salt provides a security scheme against dictionary-based attacks and attacks using precomputed lookup table like a rainbow table.

At random salt, a character / random number inserted into each character password. Suppose that salt is a character in the digits 0 .. 9, then after adding salt to password=”hello”, salted password= "1836h73e9l186l7548o23”. In case, a rule is needed to divide ascii characters into two parts, that is characters for passwords and characters for salt. So if the salt character is a numeric character, then the password is ascii characters other than numeric. If the password is only allowed in the letters of the alphabet and numbers, then salt uses ascii characters other than numbers and letters such as "", "@", "#", "$", and so on. It is intended that while authentication, salt is easy to remove.

To strengthen this salt cryptographic scheme, the chaos algorithm was added to generated the salt. With the procedure in the previous section (II.b. and II.c.), The random salt can be produced with various length and number. The code below is the chaos algorithm for salt generating in php.

```
function f($r, $x, $iterasi) {
        for ($i = 1; $i <= $iterasi; $i++) {
                $x = $r * $x * (1 - $x);
        }
        return $x;
}

function map_to($x, $nilai) {
        $n = $x;
        while ($n <= $nilai) {
                $n = $n * 10.0;
        }
        return (int)$n;    /* cropping */
}

function pangkat10($ukuran){
        $nilai = 1;
        for ($i = 1; $i < $ukuran; $i++){
                $nilai = $nilai * 10.0;
        }
        return $nilai;
}

function randomgenerator() {
        $r = 3.98716;                   // chaos variable
        $ukuran = rand(3,18);
        $x = 0.1;                       //  0<x<1
        $nilai = pangkat10($ukuran);
        $iterasi = rand(1,10000);
        $x0 = f($r, $x, $iterasi);
        $pad = map_to($x0, $nilai);
        return $pad;
}
```

C. *Authentication*

Authentication is required to ensure the originality of the radar data that is sent, so can fulfilled the authenticity of network security. Figure 5 below is the design of radar data authentication. Message digest / digital signature is generated from hashing the encrypted parameters using the MD5 algorithm and added to the encrypted radar data.

The authentication process is done by comparing the results of the transmitted data hashing with the digital signature, if the same means no changes in the transmitted data. This authentication process flow is shown in Figure 6.

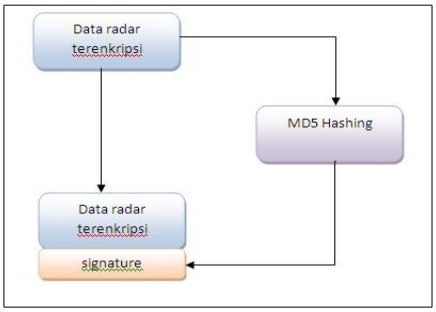

Fig. 5. Digital signature[16]

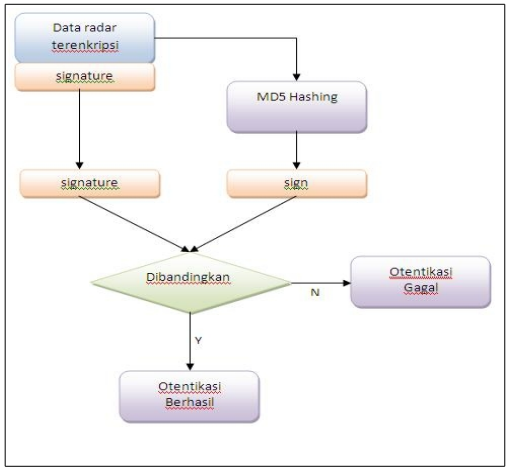

Fig. 6. The authentication[16]

IV. Result And Analysis

Surveillance radar system consists of some modules that be developed on the different language: C++, Visual Basic, and

PHP-MySQL. The security module was developed using mcrypt and openSSL library from php. Extraction module was developed using Visual Basic. The data communication via TCP/IP in VB can use the winsock component. Meanwhile, the protocol httpGet/httpPost is used to data transmission through internet or web using Inet VB component. A Salt_open.php file is created to simulate data sending that represent the *sendData()* function. It is needed to ensure the system is running properly.

In the *localhost/sender_open.php*, there are three main parts for data transmission: the data reader, the encryption, and the data sender. The encryption using mcrypt is done after the data is received into the varibles. For some data like *type* and *namaKapal*, salt cryptographic is added. The initialization is required in the first encryption steps to define the algorithm used and the output format, to generate a key using PRNG, and identity-based encryption using hash function (in this simulation using *idKapal* and *type*). Salt cryptography is inserted in the type and namaKapal variables before it is encrypted. The next process, the encrypted data is transmitted to webserver using *httppost* protocol.

Web server, as discussed in the previous section, is used to store radar data and provide information to a monitoring station. *Simpanpost.php* file is used for this function, including data decryption process before it is stored into the database. The initialization for decryption is identical with initialization for encryption, followed by decryption and salt replacing. After original data is obtained, data is saved into database.

The authentication can be implemented using digital signature addition. The code below is the making of digital signature for authentication needed. The MD5 hash function is used for this purpose.

```
$signature = MD5($key1.$emmsi.$elat.$elong.$etimeStamp.$etype.
                $enamaKapal);
```

Whereas, the code below is the authentication simulation in the server side. It is done by comparing the *$sign* parameter and the *$signature* parameter. The data originality can be obtained if these parameters are equal.

A. Computational Time Effect

The using of chaos algorithm could affect the computation time, especially the encryption time. The calculation and iteration in the chaos algorithm will consume more time and larger CPU memory than random function. Table 1 below is the comparison of processing time between the using of random and chaos algorithm for some encryption type.

Table 1. Computational time comparison

Encryption	Chaos (mS)	Random (mS)
Rijndael-256	9.451866	3.711938
TripleDES	11.070013	6.838083
Cast-128	9.780168	2.852916
Blowfish	21.916866	3.868818

All of encryption time using Chaos algorithm have been significantly increasing. The computational time also depends on the specification of computer used and the ability of server, also internet traffic off course.

B. The Security Strength

Based on the iterated experiment, sometimes the random function produces the close number. It won't be happen if it uses the chaos random number generator. The advantages are the randomness in the number and the length of number. Thus, it can make more difficult to attack the code. The other words, the chaos algorithm can strengthen the security. The code below is the result of number generator for 100 times iteration.

```
random = 406900 ; chaos = 12914
random = 10670632 ; chaos = 5110097257792522
random = 12992298 ; chaos = 865911
random = 4934115 ; chaos = 90040
random = 2525277 ; chaos = 61566165636
random = 3288726 ; chaos = 99168
random = 13211434 ; chaos = 13094813
random = 9393890 ; chaos = 4607
random = 8922082 ; chaos = 906704879349303
random = 3852468 ; chaos = 1656
random = 9984174 ; chaos = 19333638927206780
random = 7788728 ; chaos = 2804070815079
random = 13955467 ; chaos = 29208205652481
random = 8848883 ; chaos = 4507
random = 14902466 ; chaos = 61632430
random = 8815611 ; chaos = 1925503221
random = 9931858 ; chaos = 841393
random = 1005904 ; chaos = 95961492002969824
random = 13598004 ; chaos = 2643363274
random = 13565120 ; chaos = 2311
random = 12127900 ; chaos = 4702
random = 16591271 ; chaos = 8966
random = 6060505 ; chaos = 23289713392
random = 6058221 ; chaos = 580181240
random = 4280181 ; chaos = 984
random = 8674727 ; chaos = 226202618
random = 2994807 ; chaos = 932441
random = 14620750 ; chaos = 3279582500794
random = 16158227 ; chaos = 21656779283947
random = 1061849 ; chaos = 28501088193713
random = 15645007 ; chaos = 71360406926
random = 5824867 ; chaos = 6850273
random = 900062 ; chaos = 9614036755
random = 14021818 ; chaos = 69789252709769480
random = 8683580 ; chaos = 396224798
random = 5637218 ; chaos = 9822764868411136
random = 12219801 ; chaos = 97501254016756
random = 8679624 ; chaos = 19921
random = 1394036 ; chaos = 87455
random = 3475854 ; chaos = 9965300429
random = 7257032 ; chaos = 31426726952515
random = 11886846 ; chaos = 84002340922510
random = 343334 ; chaos = 659073678896
random = 5966660 ; chaos = 85765
random = 8717065 ; chaos = 14457560237
random = 2786363 ; chaos = 15315
random = 9253257 ; chaos = 237254
random = 5312294 ; chaos = 248006428932131
random = 6614148 ; chaos = 486420521
random = 3219796 ; chaos = 390613965789
random = 14057761 ; chaos = 63609169401156640
random = 10941162 ; chaos = 27071719410317
random = 15409980 ; chaos = 6440
random = 14997740 ; chaos = 996776444615738
random = 2377067 ; chaos = 64097355
random = 7475379 ; chaos = 21161347339961
random = 5885501 ; chaos = 993547097119664
random = 10532975 ; chaos = 11946973
random = 6311866 ; chaos = 994271696660431
random = 6713904 ; chaos = 13460699
random = 14295750 ; chaos = 91258
random = 6265720 ; chaos = 95423612997
random = 8207243 ; chaos = 6065469485
random = 6991801 ; chaos = 89423060897370896
random = 2877626 ; chaos = 171892347673198400
```

random = 15196347 ; chaos = 607826603038
random = 5427112 ; chaos = 377328921
random = 11562220 ; chaos = 335821
random = 16630045 ; chaos = 917787616399350
random = 13800871 ; chaos = 920619009
random = 5754439 ; chaos = 9714673005103
random = 1967676 ; chaos = 76125
random = 14255832 ; chaos = 970694
random = 10973385 ; chaos = 996784
random = 3959884 ; chaos = 428204329169973
random = 1090490 ; chaos = 5374242165
random = 9090003 ; chaos = 44057669157820504
random = 1545684 ; chaos = 380167000826449
random = 10760642 ; chaos = 9079772
random = 8513379 ; chaos = 30677
random = 8996746 ; chaos = 2814073783
random = 523929 ; chaos = 7092243066218
random = 608513 ; chaos = 57983630834689560
random = 1016217 ; chaos = 12798698612078
random = 839654 ; chaos = 7637335
random = 5722272 ; chaos = 2280845716
random = 7228425 ; chaos = 31702161859
random = 1944231 ; chaos = 1857538596
random = 6929430 ; chaos = 487104246888
random = 5723965 ; chaos = 30499933
random = 641856 ; chaos = 57200574921811
random = 4598010 ; chaos = 99417
random = 3506491 ; chaos = 397823422520
random = 3514463 ; chaos = 44789045127
random = 1631408 ; chaos = 63038957
random = 683879 ; chaos = 1171304093396816
random = 11563714 ; chaos = 9936728
random = 1868418 ; chaos = 692
random = 8091120 ; chaos = 59568
random = 10141757 ; chaos = 898404587524410

The result of random function has similar length, whereas the chaos produces more various length in output. It can be used to produce the better salt cryptographic.

V. Conclusion

Integration of security systems in radar network data communication system can be useful to secure the radar data from unauthorized parties. The selection of an efficient cryptographic algorithms in terms of speed and power can be used to scramble the radar data, although still possible an attack through traffic analysis. By adding salt cryptographic before data encryption, the encryption output will always give different codes including the encrypted code length. This will give the benefit in terms of security, because it can make more difficult to guess the data via the password dictionary (dictionary attack) and brute-force attack, include the attacks through traffic analysis, such as sniffing and Wiretapping.

All of encryption time using Chaos algorithm have been significantly increasing. The calculation and iteration in the chaos algorithm will consume more time and larger CPU memory than random function. The computational time also depends on the specification of computer used and the ability of server, also internet traffic off course. The advantage of using Chaos algorithm is the randomness of output that better than random function. So, it can be used to produce the better salt cryptographic.

Acknowledgment

We thank Research Center for Informatics - Indonesian Institute of Sciences(LIPI) and School of Electrical Engineering and Informatics-Institut Teknologi Bandung (ITB) for the facilities, advice and information they have provided.

References

[1] O.D.Winarko, A.A.Lestari, “Sistem Trigger Pada Radar Maritim INDERA,” Prosiding Seminar Radar Nasional III 2009, Bandung, 30 April 2009, ISSN: 1979-2921.

[2] W. Sediono, A.A. Lestari, “First Result of the Signal Processing of INDERA,” Prosiding Seminar Radar Nasional III 2009, Bandung, 30 April 2009, ISSN: 1979-2921.

[3] M.Wahab, “Building a Radar from The Scratch: ISRA LIPI Radar Experience,” International Conference on Telecommunication (ICTel 2009), Bandung, November 2009, pp. 171-180.

[4] O. Adeyinka, "Internet Attack Methods and Internet Security Technology," Second Asia International Conference on Modeling & Simulation, 2008 (AICMS 08) , vol., no., pp.77-82, 13-15 May 2008.

[5] N.H.Lestriandoko, “A Review Paper On Network Security For Surveillance Radar Network,” Proceeding of The 6th National Radar Seminar And The first International Conference On Radar, Antenna, Microwave, Electronics And Telecommunications (ICRAMET) 2012, Bali, April 23-24, 2012.

[6] BlueKrypt: Cryptographic Key Length Recomendation, available on http://www.keylength.com/ .

[7] N.Ferguson and B.Schneier, “Practical Cryptography,” Wiley, 2003, ISBN: 0-471-22357-3.

[8] M.Shafeeq, M.Y.Durrany, I.Afzal, “Random Key Encryption a New Cryptographic Scheme,” International Conference on Information and Emerging Technologies (ICIET) 2007, 6-7 July 2007.

[9] A.C.Sekhar, K.R.Sudha, P.V.G.D.Prasad Reddy, “Data Encryption Technique Using Random Number Generator,” IEEE International Conference on Granular Computing 2007, 2-4 November 2007.

[10] K.Marton, A.Suciu, I.Ignat, “Randomness in Digital Cryptography: A Survey,” Romanian Journal of Information Science and Technology,Vol.13, No.3, 2010, page 219-240.

[11] R.Munir, "Security Analysis of Selective Image Encryption Algorithm Based on Chaos and CBC-like Mode," 2012 7th International Conference on Telecommunication Systems, Services, and Applications (TSSA), Bali, 30-31 October 2012

[12] R.Munir, B.Riyanto, S.Sutikno, W.P.Agung, "Metode Asymmetric Watermarking pada Citra Digital Berbasiskan pada Permutasi-RC4 dan Fungsi Chaos," Seminar on Intelligent Technology and Its Applications 2008, ISBN 978-979-8897-24-5.

[13] James Lampton, “Chaos Cryptography: Protecting Data Using Chaos”, Mississippi School for Mathematics and Science.

[14] R. Clarck Robinson, “An Introduction to Dynamical Systems, Continuous and Discrete,” Pearson Prentice Hall, 2004.

[15] R.Munir, B.Riyanto, S.Sutikno, W.P.Agung, "Metode Blind Image-Watermarking Berbasis Chaos Dalam Ranah Discrete Cosine Transform (DCT)," Jurnal Ilmu Komputer Dan Teknologi Informasi, Vol III NO.2, Oktober 2003.

[16] N.H.Lestriandoko, T.Juhana, “Security System for Surveillance Radar Network Communication”, The 2nd International Conference on Radar, Antenna, Microwave, Electronics and Telecommunications (ICRAMET) 2013, Surabaya, March 27th-28th, 2013, ISSN: 1979-292