Short Research Article

Systematic Literature Review of the Role of Fuzzy Logic in the Development of Cryptographic and Steganographic Techniques

ABSTRACT

The rapid technological revolution has an impact on a variety of information security techniques. This will be important, because information can be confidential to some entities that communicate with each other. Internet in intelligent technology will be a loophole for cryptanalysts to look for information vulnerabilities. Cryptography is a method of securing data and information which is currently still supported by the development of the method. However, the data and information that are secured will still have vulnerabilities in their delivery. The combination of fuzzy logic techniques with cryptographic techniques has been applied to support the improvement of information security. This study applies a systematic literature review method, to find articles that combine the two fields. The purpose of this study is to see the development of information security techniques with a fuzzy logic approach. As a result, it is found that the development of cryptographic and steganographic techniques that utilize fuzzy logic to help improve information security. In addition, the use of fuzzy is also not limited in increasing security. Fuzzy also plays a role in selecting the best key and password and issuing random numbers from a Pseudo Random Number Generator (PRNG).

Keywords: Fuzzy, Information, Cryptography, Information System

1. INTRODUCTION

Internet technology has revolutionized rapidly. The World Wide Web, which was famous in its time, has now turned into handheld devices such as mobile phones, smartphones and sensors. The current platform supports connections between devices for the purpose of communication and data exchange.

A data communication through an open network will face various security threats and will be vulnerable to fraud. Every device that is connected to the internet, of course, already has its own standard security mechanism that is tailored to the capabilities of each device. This mechanism is an information security technique.

Kriptografi adalah sebuah bidang keilmuan yang bertujuan untuk mengamankan informasi dengan cara membuat informasi tersebut menjadi sulit dilihat dengan bantuan sebuah password atau kunci [1Techniques in cryptography are done by changing the shape of the data so that it cannot be interpreted directly [2]. Although the cryptographic results can still be viewed freely, the information is still safe because the information is random [3]. Many cryptographic algorithms have been developed to date with their advantages and

disadvantages. This aims to make it difficult for a cryptanalyst to decipher the secured information. The more difficult and increasingly random information is a challenge for developers of cryptographic methods. One technique that can help improve information security is to combine several methods into cryptographic techniques, one of which is fuzzy logic.

Fuzzy logic is an approach to problem solving that gives the degree of truth of a common true or false binary solution [1] [4]. Decision-making systems based on fuzzy logic resemble the way humans make decisions, by having a level of truth. This can be very useful in analyzing and improving the performance of cryptographic approaches on different platforms.

Combining two methods to close the gaps in one of the algorithms. This article will review the role of fuzzy methods in the field of cryptography by adopting a systematic literature review process

2. METHODOLOGY

Empirical studies in the field of computer science are currently more often used to see existing phenomena. The search in this article adopts the Systematic Literature Review technique as in [5] [6]. The review process is shown in Figure 1. The Systematic Literature Review aims to provide a comprehensive review of the current literature relevant to several problem formulations. Several articles in the field of computer science engineering adopted [5] to conduct a systematic literature review.

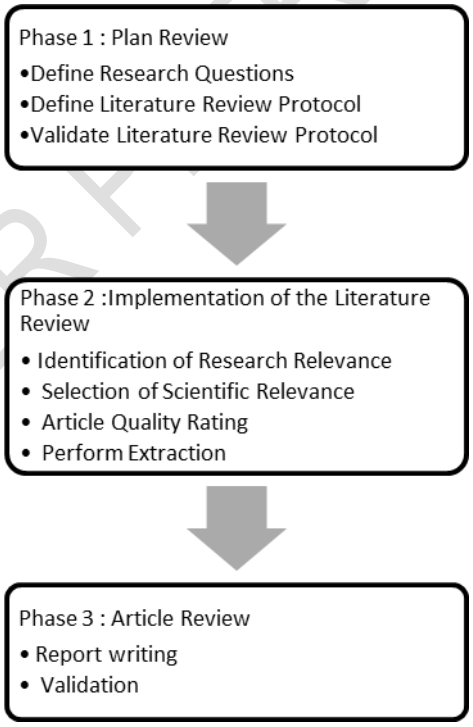

Fig. 1. Systematic Literature Review Process Flow. Adopted from [5]

The Literature Review process consists of three phases with nine activities. In the first phase, as research question 1 (RQ) is what is the role of fuzzy in cryptography? This research question is determined in the initial phase before carrying out further stages.

The literature review protocol includes the sources to be used, the period for the articles to be reviewed, the keywords to be used. The literature review protocol is shown in table 1. The sources used are research articles indexed on Google Scholar published in 2017 to 2021. This is seen because the form of further development will find the latest development of the articles obtained. Articles to be reviewed are articles published in the Journal and Proceedings.

Table 1. Systematic Literature Review Protocol

Article Published	Source	Key Word	Article Type
2017 – 2021	Google Scholar	Cryptography Fuzzy Logic	Journal and Conference

3. RESULTS AND DISCUSSION

3.1 RESULTS OF A LITERATURE SYSTEMATIC REVIEW

The literature review conducted with search keywords resulted in 13,300 articles displayed by the source. With the limitation of the year of publication of the article, 25 articles were obtained that were relevant to the research question. Table 2 shows the distribution of articles per year obtained in the literature review. And Table 3 shows the types of journal articles and proceedings articles. With the articles that are still being obtained in the literature search process, the fuzzy method plays a role in the development of cryptographic techniques.

Table 2. Article Publication Year

Publication Year	Number of Articles
2017	7
2018	8
2019	4
2020	6

Table 3. Types of Article

Articles Type	Number of Articles

Journal	10
Conference Proceeding	15

From the article extraction process, the results obtained are two clusters of fuzzy use in information security. The first cluster is that there are 21 articles that discuss the use of fuzzy in cryptography and the second cluster there are 4 articles that use fuzzy in the field of steganography. In the first cluster, the use of fuzzy in cryptography is grouped into three groups of fuzzy roles. The first is the use of fuzzy in improving information security, the second is the use of fuzzy in the issuance of keys in cryptographic techniques and the third is the use of fuzzy to issue random numbers in cryptography. Table 4 shows the results of grouping articles based on the extraction process.

Table 4. Article Extraction Results

Index	Discussion Group			
	1	2	3	4
[7]	-	Y	-	-
[8]	-	-	-	Y
[9]	-	Y	-	-
[10]	Y	-	-	-
[11]	-	Y	-	-
[12]	-	Y	-	-

[13]	-	-	Y	-
[14]	-	-	Y	-
[15]	-	Y	-	-
[16]	-	-	Y	Y
[17]	-	-	-	Y
[18]	Y	-	-	-
[19]	Y	-	-	-
[20]	-	-	Y	-
[21]	-	-	Y	-
[22]	-	-	Y	-
[23]	-	Y	-	-
[24]	-	-	-	Y
[25]	-	-	Y	-
[26]	-	-	Y	-
[27]	-	Y	-	-
[28]	-	Y	-	-

[29]	-	Y	-	-
[30]	Y	-	-	-

Group 1 discusses the use of fuzzy in the field of steganography, group 2 discusses the use of fuzzy in improving information security, group 3 discusses the use of fuzzy in issuing keys and passwords and group 4 discusses the use of fuzzy in issuing random numbers. Figure 2 shows the form of visualization of the role of fuzzy logic in the development of cryptography and steganography.

3.2 THE ROLE OF FUZZY IN CRYPTOGRAPHY

Cryptography is an information security technique that has a unique process in each stage. However, the information that is secured will still have vulnerabilities to be cracked during transmission. For this reason, fuzzy is presented to close these gaps so that it will be difficult for cryptanalysts to decipher the encoded information code

Each figure should have a caption. The caption should be concise and typed separately, not on the figure area. Figures should be self-explanatory. Information presented in the figure should not be repeated in the table. All symbols and abbreviations used in the illustrations should be defined clearly. Figure legends should be given below the figures.] A sample figure is given in figure 1.

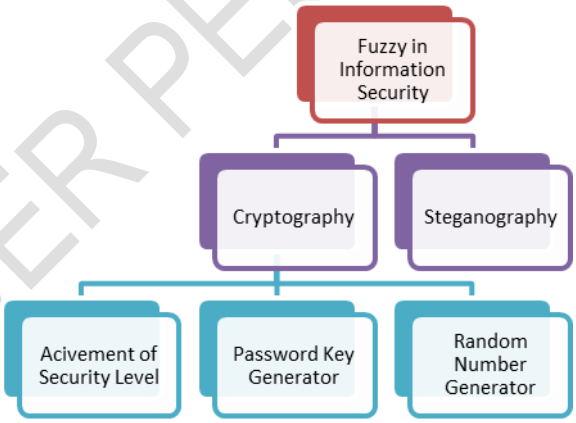

Fig. 2. The Role of Fuzzy Logic in Information Security

In the field of cryptography, fuzzy has three important roles, first is to help improve information security, second is to help issue keys and third is to help determine random numbers in pseudo random number generators (PRNG).

In the systematic search of the literature, the use of fuzzy contributes to the improvement of information security in the field of cryptography. In terms of dealing with privacy and identity breaches, the use of the proposed fuzzy logic fusion strategy can enable efficient and

accurate identification procedures for critical applications with high security [7]. Fuzzy is also used in the development of new techniques in Privacy Preserving Data Mining (PPDM) related to data privacy issues in the mining process, in this case fuzzy contributes to improving data security in cryptographic techniques [12]. Security of messages through transmission media also utilizes fuzzy as additional security [9]. The use of fuzzy is proposed to assist accuracy in biometric recognition in the realm of information security, fuzzy can provide a better level of accuracy [29].

In terms of algorithm hybridization, fuzzy is used to optimize information security in the RSA algorithm [11]. Fuzzy is also used to see the optimization of information security in the AES algorithm and lightweight AES [15]. Information security enhancement using fuzzy is also combined with an artificial neural network autoencoder [23]. The use of Boolean XOR gates is also integrated [27] and the use of elliptic curves [28] to improve the security of the encoded information.

Keys and Passwords in cryptography have an important role in securing information. This key selection thing is something that is hard to do. In this case, fuzzy has a role to assist in selecting the best key to improve information security. Euclid's and fuzzy theorems are combined to perform key publications which ultimately show better evaluation results [14]. In terms of key delivery, fuzzy is also used to secure keys that are transmitted through wireless sensor network devices [21]. Fuzzy is also combined with the Diffie Helman technique to secure the key sent to the recipient [22].

Symmetric cryptographic algorithms will use the same key to encrypt and decrypt information. A vulnerability will occur if the use of the same key is used to secure information in multiple sessions. The use of fuzzy helps increase convenience for users through the issuance of stream-based key ciphers [20]. Key quality is also assisted using fuzzy combined with the process of combining session keys and random keys [26] [25].

Improving the performance of cryptographic techniques is also supported using a random number generated from a pseudo random number generator (PRNG). Fuzzy is used to increase the strength of random numbers by changing the member function [24]. The fuzzy approach in PRNG was also developed in the modeling [17]. To generate better random values, PRNG is proposed to adopt fuzzy coquet integral [16]. The addition of the LSFR process in the PRNG also uses fuzzy as a number regulator, this also improves the quality of the generated random numbers [24].

3.2 THE ROLE OF FUZZY IN STEGANOGRAPHY

Information security does not only use cryptographic techniques, but steganography techniques also help secure information by inserting it into a digital object known as the insertion media. Fuzzy has several roles in helping secure information using steganography techniques.

To increase the number of messages that can be hidden, fuzzy is used to help detect image edges with the chaotic method [10]. Medical image security also utilizes fuzzy to insert proprietary information by utilizing image edges [18]. The approach with fuzzy in image edge detection is proposed to be combined with LSB technique to increase the number of messages that can be inserted [19]. In addition to image objects, objects in the form of audio files are also used as storage media. The use of fuzzy in the insertion of audio files is also used to detect free space and help better spread [30]. The fuzzy approach can increase up to 48% of the PSNR quality of the audio file that has been filled with messages.

4. CONCLUSION

Information security is a unique and difficult thing, although many algorithms are built, weaknesses and loopholes will always remain. The use of fuzzy in information security helps improve performance in information security. Fuzzy has another role in the world of cryptography, which is to function as an approach that can help in key issuance and improve the quality of random numbers in PRNGs. In addition, fuzzy also plays a role in securing information using steganography techniques. Thus, the systematic search of this literature contributes to designing the use of fuzzy in other techniques for information security.

REFERENCES

[1] S. B. Sadkhan and A. O. Salman, "Fuzzy Logic for Performance Analysis of AES and Lightweight AES," Kurdistan Region, Iraq, 2018.

[2] E. Ardhianto, A. Trisetyarso, W. Suparta, B. S. Abbas and C. H. Kang, "Design Securing Online Payment Transactions Using Stegblock Through Network Layers," in 3rd International Conference on Informatics, Engineering, Science, and Technology (INCITEST 2020) , Bandung, Indonesia, 2020.

[3] E. Ardhianto, H. L. H. S. Warnanrs, B. Soewito, F. L. Gaol and E. Abdurrachman, "Improvement of Steganography Technique: A Survey," in 1st International Multidisciplinary Conference on Education, Technology, and Engineering (IMCETE 2019), Serang, Indonesia, 2019.

[4] P. Sethuraman, P. S. Tamizharasan and K. Arputharaj, "Fuzzy Genetic Elliptic Curve Dife Hellman Algorithm for Secured Communication in Networks," Wireless Personal Communications, vol. 105, no. 3, p. 993–1007, 2019.

[5] P. Brereton, B. . A. Kitchenham, D. Budgen, M. Turner and M. Khalil, "Lessons from applying the systematic literature review process within the software engineering domain," Journal of Systems and Software, vol. 80, no. 4, pp. 571-583, 2007.

[6] A. A. Soofi, M. I. Khan and F. E. Amin, "A Review on Data Security in Cloud Computing," International Journal of Computer Applications , vol. 94, no. 5, pp. 12-20, 2014.

[7] M. . M. Eid and M. A. Mohamed, "A Secure Multimodal Authentication System Based on Chaos Cryptography and Fuzzy Fusion of Iris and Face," in 2017 Intl Conf on Advanced Control Circuits Systems (ACCS) Systems & 2017 Intl Conf on New Paradigms in Electronics & Information Technology (PEIT), Alexandria, Egypt, 2017.

[8] A. I. V and K. Alnajjar, "Correlation Immune Pseudo-random Number Generator Based on Fuzzy Logic," in 2017 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM) , St. Petersburg, 2017.

[9] M. Muthumeenakshi, T. Archana and P. Muralikrishna, "FUZZY APPLICATION IN SECURED DATA TRANSMISSION," International Journal of Pure and Applied Mathematics, pp. 711-715, 2017.

[10] C. Vanmathi and S. Prabu, "Image Steganography Using Fuzzy Logic and Chaotic for Large Payload and High Imperceptibility," International Journal of Fuzzy Systems, p. 460–473, 2017.

[11] K. Abdullah, S. A. Bakar, N. H. Kamis and H. Aliamis, "RSA Cryptosystem with Fuzzy Set Theory for Encryption and Decryption," in 13th IMT-GT International Conference on Mathematics, Statistics and their Applications (ICMSA2017), Kedah, Malaysia, 2017.

[12] M. BANSAL, D. GROVER and D. SHARMA, "SECURE MINING AND SHARING OF FINANCIAL DATA: FUZZY LOGIC AND CRYPTOGRAPHY," Indian Journal of Computer Science and Engineering (IJCSE), pp. 542-547, 2017.

[13] P. Tubthong and V. Suttichaya, "The Fuzzy Scheduling Algorithm for the Parallel Key Searching Problem on Cloud Environment," in 21st International Computer Science and Engineering Conference, Bangkok, Thailand, 2017.

[14] R. Sailaja, C. Rupa and A. S. Chakravarthy, "A novel integrated approach using Euclid's and fuzzy logic for secure communication," Int. J. Information Privacy, Security and Integrity, pp. 253-267, 2018.

[15] S. B. Sadkhan and A. O. Salman, "Fuzzy Logic for Performance Analysis of AES and Lightweight AES," in 2018 International Conference on Advanced Science and Engineering (ICOASE), Kurdistan Region, Iraq, 2018.

[16] S. E. El-Khamy and A. G. Mohamed, "Image Keyed PN Sequence Generator and Authentication Technique Based on Choquet Fuzzy Integral," in 35th NATIONAL RADIO SCIENCE CONFERENCE (NRSC 2018), Cairo, Egypt, 2018.

[17] N. Nguyen, G. Kaddoum and F. Gagnon, "Implementation of a Chaotic True Random Number Generator Based on Fuzzy Modeling," in 16th IEEE International New Circuits and Systems Conference (NEWCAS), Montreal, QC, Canada, 2018.

[18] T. Yuvaraja and R. S. Sabeenian, "Performance analysis of medical image security using steganography based on fuzzy logic," Cluster Computing, pp. 1-7, 2018.

[19] H. S. Yusuf and H. Hagras, "Towards Image Steganography Using Type-2 Fuzzy Logic and Edge Detection," in 10th Computer Science and Electronic Engineering (CEEC), Colchester, UK, 2018.

[20] K. Vetrivel, S. Shanmugam and S. Gurumurthy, "Extending Network Security by Multi Model Encryption Standards for Dynamic Networks Using Fuzzy Logic Technique," in Sri Padmavati Mahila Visvavidyalayam (SPMVV), 2018 IADS International Conference on Computing, Communications & Data Engineering (CCODE) , Andhra Pradesh, India, 2018.

[21] M. . S. Yousefpoor and H. Barati, "DSKMS: a dynamic smart key management system based on fuzzy logic in wireless sensor networks," Wireless Networks, pp. 1-21, 2018.

[22] P. Sethuraman, P. S. Tamizharasan and K. Arputharaj, "Fuzzy Genetic Elliptic Curve Dife Hellman Algorithm for Secured Communication in Networks," Wireless Personal Communications, pp. 1-15, 2019.

[23] S. Pattanayak and S. A. Ludwig, "Improving Data Privacy Using Fuzzy Logic and Autoencoder Neural Network," in 2019 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE), New Orleans, LA, USA, 2019.

[24] I. . V. Anikin and K. Alnajjar, "Increasing the quality of pseudo-random number generator based on fuzzy logic," Samara, Russian Federation, 2019.

[25] A. Bhowmik, S. Karforma, . J. Dey and A. Sarkar, "Fuzzy-Based Session Key as Restorative Fuzzy-Based Session Key as Restorative for Secured Wireless Communication," Haldia, India, 2020.

[26] A. Bhowmik and S. Karforma, "A Key Generation technique using Concept of Recurrence Relation and Fuzzy logic against Security Breach in Wireless Communication," 2020.

[27] R. Chemlal, "A note on combining chaotic dynamical systems using the fuzzy logic XOR operator," 2020.

[28] G. Singh and S. Garg, "Fuzzy Elliptic Curve Cryptography based Cipher Text Policy Attribute based Encryption for Cloud Security," London, UK, 2020.

[29] K. K. SINGH and S. BARDE, "FUZZY LOGIC IN TERMS OF BIOMETRICS," i-manager's Journal on Image Processing, vol. 7, no. 4, pp. 17-22, 2020.

[30] M. . M. Amrulloh and T. Ahmad, "Utilizing Fuzzy Logic in Developing Reversible Data Hiding Method," International Journal of Intelligent Engineering and Systems,, vol. 13, no. 5, pp. 327-336, 2020.