

1  
2  
3  
4  
5  
6  
7  
8  
9  
10

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

11  
12

---

## ABSTRACT

The rapid technological revolution had 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 logic is also not limited to increasing security. Fuzzy logic also plays a role in selecting the best key and password and issuing random numbers from a Pseudo-Random Number Generator (PRNG).

13  
14  
15  
16

*Keywords: Fuzzy, Information, Cryptography, Information System*

17  
18

## 1. INTRODUCTION

19  
20  
21  
22  
23  
24  
25

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 communication and data exchange. 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 standard security mechanism that is tailored to the capabilities of each device. This mechanism is an information security technique.

26  
27  
28  
29  
30  
31  
32  
33

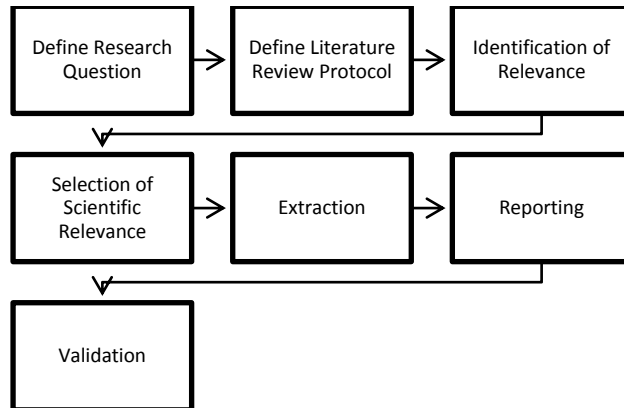
Cryptography is a scientific field that aims to become information by making the information difficult to see with the help of a password or key [1]. Techniques in cryptography are done by changing the shape of the data so that it cannot be interpreted directly [2]. Although the cryptographic results 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

34 information security is to combine several methods into cryptographic techniques, one of  
 35 which is fuzzy logic.

36 Fuzzy logic is an approach to problem-solving that gives the degree of truth of a common  
 37 true or false binary solution [1] [4]. Decision-making systems based on fuzzy logic resemble  
 38 the way humans make decisions, by having a level of truth. This can be very useful in  
 39 analyzing and improving the performance of cryptographic approaches on different  
 40 platforms. This article will review the role of fuzzy logic methods in the field of cryptography  
 41 by adopting a systematic literature review process

42  
 43 **2. METHODOLOGY**  
 44

45 Empirical studies in the field of computer science are currently more often used to see  
 46 existing phenomena. The search in this article adopts the Systematic Literature Review  
 47 technique as in [5] [6]. The review process is shown in Fig. 1. The Systematic Literature  
 48 Review aims to provide a comprehensive review of the current literature relevant to several  
 49 problem formulations. Several articles in the field of computer science engineering adopted  
 50 [5] to conduct a systematic literature review.  
 51



52  
 53 **Fig. 1. Systematic Literature Review Process Flow. Adopted from [5]**  
 54

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

58 The literature review protocol includes the sources to be used, the period for the articles to  
 59 be reviewed, the keywords to be used. The literature review protocol is shown in table 1. The  
 60 sources used are research articles indexed on Google Scholar published from 2017 to 2021.  
 61 This is seen because the form of further development will find the latest development of the  
 62 articles obtained. Articles to be reviewed are articles published in the Journal and  
 63 Proceedings.  
 64

65 **Table 1. Systematic Literature Review Protocol**  
 66

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

67

### 68 3. RESULTS AND DISCUSSION

69

#### 70 3.1 RESULTS OF A LITERATURE SYSTEMATIC REVIEW

71

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

78

79 **Table 2. Article Publication Year**

80

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

81

82

83 **Table 3. Types of Articles**

84

Articles Type	Number of Articles
Journal	10
Conference Proceeding	15

85

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

94

95 **Table 4. Article Extraction Results**

96

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	-	-	-

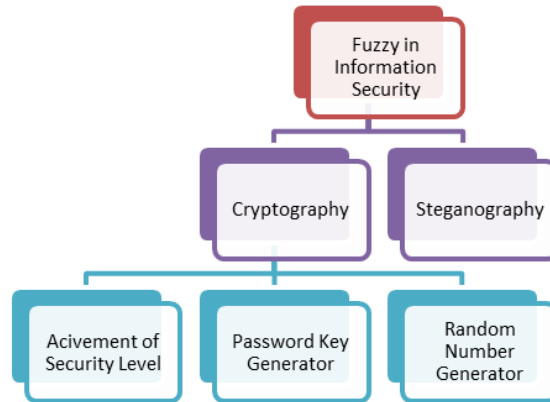
---

97  
98  
99  
100  
101  
102  
103  
104  
105  
106  
107  
108  
109

Group 1 discusses the use of fuzzy logic in the field of steganography, group 2 discusses the use of fuzzy logic in improving information security, group 3 discusses the use of fuzzy logic in issuing keys and passwords and group 4 discusses the use of fuzzy logic 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 logic is presented to close these gaps so that it will be difficult for cryptanalysts to decipher the encoded information code.



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

110  
111  
112  
113  
114  
115  
116  
117  
118  
119  
120  
121  
122  
123  
124  
125  
126  
127  
128  
129  
130  
131  
132  
133  
134  
135  
136  
137  
138  
139  
140  
141  
142  
143  
144  
145  
146  
147  
148  
149  
150

In the field of cryptography, fuzzy logic 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 logic 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 logic contributes to improving data security in cryptographic techniques [12]. Security of messages through transmission media also utilizes fuzzy logic as additional security [9]. The use of fuzzy logic is proposed to assist accuracy in biometric recognition in the realm of information security, fuzzy logic can provide a better level of accuracy [29].

In terms of algorithm hybridization, fuzzy logic is used to optimize information security in the RSA algorithm [11]. Fuzzy logic is also used to see the optimization of information security in the AES algorithm and lightweight AES [15]. Information security enhancement using fuzzy logic 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 hard to do. In this case, fuzzy logic has a role to assist in selecting the best key to improve information security. Euclid's and fuzzy logic theorems are combined to perform key publications which ultimately show better evaluation results [14]. In terms of key delivery, fuzzy logic is also used to secure keys that are transmitted through wireless sensor network devices [21]. Fuzzy logic 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 logic helps increase convenience for users through the issuance of stream-based key ciphers [20]. The key quality is also assisted using fuzzy logic 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 logic is used to

151 increase the strength of random numbers by changing the member function [24]. The fuzzy  
152 logic approach in PRNG was also developed in the modeling [17]. To generate better  
153 random values, PRNG is proposed to adopt a fuzzy coquet integral [16]. The addition of the  
154 LFSR process in the PRNG also uses fuzzy as a number regulator, this also improves the  
155 quality of the generated random numbers [24].

156

### 157 **3.2 THE ROLE OF FUZZY IN STEGANOGRAPHY**

158

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

163

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

173

174

### 175 **4. CONCLUSION**

176

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

185

### 186 **REFERENCES**

187

188 [1] S. B. Sadkhan and A. O. Salman, "Fuzzy Logic for Performance Analysis of AES  
189 and Lightweight AES," Kurdistan Region, Iraq, 2018.

190 [2] E. Ardianto, A. Trisetyarso, W. Suparta, B. S. Abbas and C. H. Kang, "Design  
191 Securing Online Payment Transactions Using Stegblock Through Network Layers,"  
192 in 3rd International Conference on Informatics, Engineering, Science, and  
193 Technology (INCITEST 2020) , Bandung, Indonesia, 2020.

194 [3] E. Ardianto, H. L. H. S. Warnanrs, B. Soewito, F. L. Gaol and E. Abdurrachman,  
195 "Improvement of Steganography Technique: A Survey," in 1st International  
196 Multidisciplinary Conference on Education, Technology, and Engineering (IMCETE  
197 2019), Serang, Indonesia, 2019.

198 [4] P. Sethuraman, P. S. Tamizharasan and K. Arputharaj, "Fuzzy Genetic Elliptic Curve  
199 Dife Hellman Algorithm for Secured Communication in Networks," Wireless Personal  
200 Communications, vol. 105, no. 3, p. 993–1007, 2019.

- 201 [5] P. Brereton, B. . A. Kitchenham, D. Budgen, M. Turner and M. Khalil, "Lessons from  
202 applying the systematic literature review process within the software engineering  
203 domain," *Journal of Systems and Software*, vol. 80, no. 4, pp. 571-583, 2007.
- 204 [6] A. A. Soofi, M. I. Khan and F. E. Amin, "A Review on Data Security in Cloud  
205 Computing," *International Journal of Computer Applications* , vol. 94, no. 5, pp. 12-  
206 20, 2014.
- 207 [7] M. . M. Eid and M. A. Mohamed, "A Secure Multimodal Authentication System  
208 Based on Chaos Cryptography and Fuzzy Fusion of Iris and Face," in 2017 Intl Conf  
209 on Advanced Control Circuits Systems (ACCS) Systems & 2017 Intl Conf on New  
210 Paradigms in Electronics & Information Technology (PEIT), Alexandria, Egypt, 2017.
- 211 [8] A. I. V and K. Alnajjar, "Correlation Immune Pseudo-random Number Generator  
212 Based on Fuzzy Logic," in 2017 International Conference on Industrial Engineering,  
213 Applications and Manufacturing (ICIEAM) , St. Petersburg, 2017.
- 214 [9] M. Muthumeenakshi, T. Archana and P. Muralikrishna, "FUZZY APPLICATION IN  
215 SECURED DATA TRANSMISSION," *International Journal of Pure and Applied  
216 Mathematics*, pp. 711-715, 2017.
- 217 [10] C. Vanmathi and S. Prabu, "Image Steganography Using Fuzzy Logic and Chaotic  
218 for Large Payload and High Imperceptibility," *International Journal of Fuzzy  
219 Systems*, p. 460–473, 2017.
- 220 [11] K. Abdullah, S. A. Bakar, N. H. Kamis and H. Aliamis, "RSA Cryptosystem with  
221 Fuzzy Set Theory for Encryption and Decryption," in 13th IMT-GT International  
222 Conference on Mathematics, Statistics and their Applications (ICMSA2017), Kedah,  
223 Malaysia, 2017.
- 224 [12] M. BANSAL, D. GROVER and D. SHARMA, "SECURE MINING AND SHARING OF  
225 FINANCIAL DATA: FUZZY LOGIC AND CRYPTOGRAPHY," *Indian Journal of  
226 Computer Science and Engineering (IJCSE)*, pp. 542-547, 2017.
- 227 [13] P. Tubthong and V. Suttichaya, "The Fuzzy Scheduling Algorithm for the Parallel  
228 Key Searching Problem on Cloud Environment," in 21st International Computer  
229 Science and Engineering Conference, Bangkok, Thailand, 2017.
- 230 [14] R. Sailaja, C. Rupa and A. S. Chakravarthy, "A novel integrated approach using  
231 Euclid's and fuzzy logic for secure communication," *Int. J. Information Privacy,  
232 Security and Integrity*, pp. 253-267, 2018.
- 233 [15] S. B. Sadkhan and A. O. Salman, "Fuzzy Logic for Performance Analysis of AES  
234 and Lightweight AES," in 2018 International Conference on Advanced Science and  
235 Engineering (ICOASE), Kurdistan Region, Iraq, 2018.
- 236 [16] S. E. El-Khamy and A. G. Mohamed, "Image Keyed PN Sequence Generator and  
237 Authentication Technique Based on Choquet Fuzzy Integral," in 35th NATIONAL  
238 RADIO SCIENCE CONFERENCE (NRSC 2018), Cairo, Egypt, 2018.
- 239 [17] N. Nguyen, G. Kaddoum and F. Gagnon, "Implementation of a Chaotic True  
240 Random Number Generator Based on Fuzzy Modeling," in 16th IEEE International  
241 New Circuits and Systems Conference (NEWCAS), Montreal, QC, Canada, 2018.

- 242 [18] T. Yuvaraja and R. S. Sabeenian, "Performance analysis of medical image security  
243 using steganography based on fuzzy logic," Cluster Computing, pp. 1-7, 2018.
- 244 [19] H. S. Yusuf and H. Hagra, "Towards Image Steganography Using Type-2 Fuzzy  
245 Logic and Edge Detection," in 10th Computer Science and Electronic Engineering  
246 (CEECE), Colchester, UK, 2018.
- 247 [20] K. Vetrivel, S. Shanmugam and S. Gurumurthy, "Extending Network Security by  
248 Multi Model Encryption Standards for Dynamic Networks Using Fuzzy Logic  
249 Technique," in Sri Padmavati Mahila Visvavidyalayam (SPMVV), 2018 IADS  
250 International Conference on Computing, Communications & Data Engineering  
251 (CCODE) , Andhra Pradesh, India, 2018.
- 252 [21] M. . S. Yousefpoor and H. Barati, "DSKMS: a dynamic smart key management  
253 system based on fuzzy logic in wireless sensor networks," Wireless Networks, pp. 1-  
254 21, 2018.
- 255 [22] P. Sethuraman, P. S. Tamizharasan and K. Arputharaj, "Fuzzy Genetic Elliptic Curve  
256 Diffe Hellman Algorithm for Secured Communication in Networks," Wireless Personal  
257 Communications, pp. 1-15, 2019.
- 258 [23] S. Pattanayak and S. A. Ludwig, "Improving Data Privacy Using Fuzzy Logic and  
259 Autoencoder Neural Network," in 2019 IEEE International Conference on Fuzzy  
260 Systems (FUZZ-IEEE), New Orleans, LA, USA, 2019.
- 261 [24] I. . V. Anikin and K. Alnajjar, "Increasing the quality of pseudo-random number  
262 generator based on fuzzy logic," Samara, Russian Federation, 2019.
- 263 [25] A. Bhowmik, S. Karforma, . J. Dey and A. Sarkar, "Fuzzy-Based Session Key as  
264 Restorative Fuzzy-Based Session Key as Restorative for Secured Wireless  
265 Communication," Haldia, India, 2020.
- 266 [26] A. Bhowmik and S. Karforma, "A Key Generation technique using Concept of  
267 Recurrence Relation and Fuzzy logic against Security Breach in Wireless  
268 Communication," 2020.
- 269 [27] R. Chemlal, "A note on combining chaotic dynamical systems using the fuzzy logic  
270 XOR operator," 2020.
- 271 [28] G. Singh and S. Garg, "Fuzzy Elliptic Curve Cryptography based Cipher Text Policy  
272 Attribute based Encryption for Cloud Security," London, UK, 2020.
- 273 [29] K. K. SINGH and S. BARDE, "FUZZY LOGIC IN TERMS OF BIOMETRICS," i-  
274 manager's Journal on Image Processing, vol. 7, no. 4, pp. 17-22, 2020.
- 275 [30] M. . M. Amrulloh and T. Ahmad, "Utilizing Fuzzy Logic in Developing Reversible  
276 Data Hiding Method," International Journal of Intelligent Engineering and Systems,,  
277 vol. 13, no. 5, pp. 327-336, 2020.

278