A novel secure artificial bee colony with advanced encryption standard technique for biomedical signal processing

Brwa Khalil Abdullah Ahmed1, Rasha Dheyaa Mahdi2, Tarek Ismail Mohamed3, Refed Adnan Jaleel4, Mohanad Ahmed Salih5, Musaddak Maher Abdul Zahra6a,b

1Shaqlawa technical college, Erbil polytechnic University, Management Information System, Iraq
2Technical Engineering Collage, Northern Technical University (NTU), Mosul, Iraq
3College of Mass Communication, Ajman University, Ajman, U.A.E
4Dept. of Information & Communication Engineering, Al-Nahrain University, Iraq
5Dept. of Computer Science, Al-Anbar University, Iraq
6a Dept. of Computer Tech. Engineering, Al-Mustaqbal University College, Iraq
6b Dept. of Electrical Engineering, University of Babylon, Iraq

ABSTRACT

Over the years, the privacy of a biomedical signal processing is protected using the encryption techniques design and meta-heuristic algorithms which are significant domain and it will be more significant shortly. Present biomedical signal processing research contained security because of their critical role in any developing technology that contains applications of cryptography and health deployment. Furthermore, implementing public-key cryptography in biomedical signal processing sequence testing equipment needs a high level of skill. Whatever key is being broken with enough computing capabilities using brute-force attack. As a result, developing a biomedical signal processing cryptography model is critical for improving the connection between existing and emerging technology. Furthermore, public-key cryptography implementation for meta-heuristic-based biomedical signal processing sequence test equipment necessitates a high level of skill. The suggested novel technique can be used to develop a secure algorithm of artificial bee colony, which depend on the advanced encryption standard (AES). AES can be used to reduce the encryption time and to increase the protection capacity for health systems. The novel secure can protect the biomedical signal processing against plain text attacks.

Keywords: AES, ABC, BSP, Encryption, Optimization

Corresponding Author:
Refed Adnan Jaleel
Information and Communication Engineering
Al-Nahrain University
Baghdad, Iraq
E-mail: Iraq_it_2010@yahoo.com

1. Introduction

The science of protecting the information of communications and messages is known as cryptography. The other sub discipline, cryptanalysis, aims to undermine or overcome cryptography's security [1] [2]. Cryptanalysis and cryptography are built on the foundation of mathematics. Cryptography is most usually connected with encryption, which is the process of transforming information and data into a format that is inaccessible to anybody who is not permitted to see it. In the most industrialized countries and areas, the population of middle-aged and elderly individuals predominates, necessitating government intervention to address health-care issues [3] [4]. This leads in a shortage of working adults to care for the growing senior population, potentially causing financial problems while also lengthening the time it takes for a patient to obtain treatment [5] [6]. As a result, newer solutions are needed to improve the level of automation from current
systems and to handle the massive amounts of data generated, stored, and sent between them in a safe and efficient manner. [7] [8]. In this paper, the field of AES using ABC for biomedical signal processing is suggested, it encompasses the measurement and digitization of patient monitoring such as the transmission of packets over a wireless network and the delivery of medical data to health-care experts, as well as blood pressure and electrocardiograms (ECGs). The study aims to build a novel secure technique incorporating biomedical signal, the AES algorithm which implemented and integrated with the biological environment, and artificial bee colony. By generating primary key and rule keys, this technique can protect biological signals sent through optimal healthcare systems platforms from plain text attacks. The study makes several achievements, including (I) the algorithm of multilayer encryption that integrates the algorithm of AES, and biomedical signal processing, (ii) an encryption technique which is reliable for the systems of artificial bee colony-based healthcare, (iii) a technique of encryption that reduces the message length of ECG and thus reduces complicated mathematical operations, (iv) the technique of encryption that enhances the encryption power and offers better security and much more complex to the multilayer ABC and AES.

2. Material and methods

2.1. Biomedical Signal Processing

Bio-medical signal processing is primarily concerned with the novel applications of the methods of processing signals to biomedical signals via numerous innovative collaborations of biomedical knowledge with the method [9]. It is indeed a fast-growing field with numerous applications [10]. These vary from the development of artificial limbs and assistive devices for the disabled to the creation of advanced systems of medical monitoring which can perform noninvasively to provide real-time views of human body workings [11]. There are different kinds of common used medical systems. Ultrasound, pylethesmography, and electrocardiography are all utilized for a variety of reasons. Figure 1 depicts the stages of biosignal processing [12].

![Figure 1. Block diagram of the general biomedical signal processing](image-url)
2.2. Artificial bee colony
In 2005, Karaboga proposed the algorithm of Artificial Bee Colony (ABC) for enhancing numeric problems. The algorithm's authors, along with some researchers, provided many such developments [13] [14]. The ABC algorithm is based on honey bee swarms that represent bee swarms' intelligent foraging actions. It is a stochastic optimization algorithm that is population based, very simple, and robust. A honey bees' swarm could complete tasks successfully by social cooperation [15]. Three types of bees in the ABC algorithm: scout bees, onlooker bees, and employed bees. The food searching around the source of food throughout their memory is in the employed bees, while onlooker bees exchange information about that food sources [16]. Onlooker bees goal is to select better food sources among employed bees sources discovered [17]. The food source with higher quality (fitness) will be chosen over the one with lower quality by onlooker bees [18]. According to the ABC algorithm, the employed bees is the first half of the swarm, while the second half is made up of onlooker bees. the derived from a small number of employed bees is the scout bees that are let down the sources of food in discovery of better ones. This is clear from the ABC algorithm's general flow chart (depict in Figure 2) [17].

![Flowchart of ABC algorithm](image)

Figure 2. Flowchart of ABC algorithm

2.3. Advanced encryption standard
AES was a top contender in the NIST competing and was named the most strong encryption algorithm in October 2000 [19] [20]. It is also recognized as Rijndael and has a variable key length of 256 bits, 192 bits, or 128 bits with 128 bits fixed-block size [21] [22]. AES is an algorithm which is symmetric with a private key that is used for encryption/decryption processes. Each round of AES encryption-decryption processes consists of four basic stages. ShiftRows is the permutation stage, and the remaining are three substitution stages that are byte Substitute, MixColumn, and AddRundKey [23] [24]. Figure 3 depicts the Advanced Encryption Standard algorithm's encryption and decryption procedures [25].
3. Results and discussion

Researchers in the field of biomedical research have access to an ever-expanding database of digital recordings of biological signals and related data. Encryption quality are all included in the experimental analysis. This is the most important test for demonstrating the given algorithm’s good security. The encryption and decryption throughput of algorithms without and with ABC can be calculated using encryption and decryption time. The algorithm’s taken time for encrypt/decrypt inputted ECG signals is one of the performance parameters. A total of 20 experiments were conducted to ensure that no one participant’s results were influenced by their own bias. Table 1 offers the decryption and encryption execution time with ABC and without ABC. Figures of the ECG shown in Figure 4 and Figure 5 for original signal and cipher signal.

Table 1. Time of encryption and decryption

<table>
<thead>
<tr>
<th>Number of rounds</th>
<th>AES</th>
<th>AES</th>
<th>AES with ABC</th>
<th>AES with ABC</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Encryption Time</td>
<td>Decryption Time</td>
<td>Encryption Time</td>
<td>Decryption Time</td>
</tr>
<tr>
<td>1</td>
<td>30.44</td>
<td>45.87</td>
<td>20.99</td>
<td>32.84</td>
</tr>
<tr>
<td>2</td>
<td>27.21</td>
<td>43.22</td>
<td>19.22</td>
<td>30.29</td>
</tr>
<tr>
<td>3</td>
<td>27.22</td>
<td>44.10</td>
<td>19.21</td>
<td>31.64</td>
</tr>
<tr>
<td>4</td>
<td>26.13</td>
<td>42.76</td>
<td>18.22</td>
<td>29.21</td>
</tr>
<tr>
<td>5</td>
<td>26.27</td>
<td>40.13</td>
<td>17.99</td>
<td>27.54</td>
</tr>
<tr>
<td>6</td>
<td>26.55</td>
<td>40.14</td>
<td>17.87</td>
<td>27.23</td>
</tr>
<tr>
<td>7</td>
<td>25.11</td>
<td>39.24</td>
<td>16.98</td>
<td>26.55</td>
</tr>
<tr>
<td>8</td>
<td>29.29</td>
<td>45.88</td>
<td>20.25</td>
<td>32.76</td>
</tr>
<tr>
<td>9</td>
<td>24.87</td>
<td>38.41</td>
<td>17.23</td>
<td>25.22</td>
</tr>
<tr>
<td>10</td>
<td>31.56</td>
<td>47.24</td>
<td>22.78</td>
<td>39.35</td>
</tr>
<tr>
<td>11</td>
<td>22.12</td>
<td>34.11</td>
<td>12.48</td>
<td>29.44</td>
</tr>
<tr>
<td>12</td>
<td>22.58</td>
<td>34.78</td>
<td>12.22</td>
<td>29.82</td>
</tr>
<tr>
<td>13</td>
<td>23.69</td>
<td>35.99</td>
<td>14.77</td>
<td>30.25</td>
</tr>
<tr>
<td>14</td>
<td>22.11</td>
<td>35.89</td>
<td>12.24</td>
<td>30.12</td>
</tr>
</tbody>
</table>
4. Conclusions

This study presents a novel secure technique incorporating ABC and AES algorithm for biomedical signal processing, which reduces the message length of biomedical signal and the complicated mathematical operations which use much more resources and took a more processing time. A novel technique employs keys provided by AES standards that enhances the power of encryption while also providing increased complexity and security. The needed breaking time of decryption has been significantly increased. The concepts of AES and ABC computing combination improves the encryption and decryption procedures. The results indicate that combining ABC and AES outperforms the original algorithm of AES. Experiment results show that a novel technique gives a high-level of integrity, security, robustness, and efficiency. In fact, the field of joint encryption is ripe for investigation.
References


