Metaheuristic secured transmission in Telecare Medical Information System (TMIS) in the face of post-COVID-19

Joydeep Dey¹ · Arindam Sarkar² · Sunil Karforma³ · Bappaditya Chowdhury⁴

Received: 18 February 2021 / Accepted: 23 September 2021

© The Author(s), under exclusive licence to Springer-Verlag GmbH Germany, part of Springer Nature 2021

Abstract

The outbreak of novel corona virus had led the entire world to make severe changes. A secured healthcare data transmission has been proposed through Telecare Medical Information System (TMIS) based on metaheuristic salp swarm. Patients need proper medical remote treatments in this Post-COVID-19 time from their quarantines. Secured transmission of medical data is a significant challenge of digitally overwhelmed environment. The objective is to impart the patients' data by encryption with confidentiality and integrity. Eavesdroppers can carry sniffing and spoofing in order to deluge the data. In this paper, a novel scheme on metaheuristic salp swarm based intelligence has been sculptured to encrypt electrocardiograms (ECG) for data privacy. Metaheuristic approach has been blended in cryptographic engineering to address the TMIS security issues. Session key has been derived from the weight vector of the fittest salp from the salp population. The exploration and exploitation control the movements of the salps. The proposed technique baffles the eavesdroppers by the key strength and other robustness factors. The results, thus obtained, were compared with some existing classical techniques with benchmark results. The proposed MSE and RMSE were 28,967.85, and 81.17 respectively. The time needed to decode 128 bits proposed session key was 8.66×10^{52} years. The proposed cryptographic time was 8.8 s.

Keywords COVID-19 · Telecare Medical Information System (TMIS) · ECG · Salp swarm · Session key

1 Introduction

The novel corona virus (COVID-19) pandemic has put the entire world into turmoil, involving all spheres of life. COVID-19 is caused by SARS-CoV-2 virus and transmitting exponentially. Telecare Medical Information System (TMIS) is the technology friendly support system which provides enhanced treatment facilities to patients in this global COVID-19 pandemic era. There exists an incredible impact on the human society on account of COVID-19. The patients belonging from remote areas face too much

difficulty in accessing the basic health care facilities for their sustainability due lockdown, containment zones, self isolation, etc. Patients unable to visit the hospitals physically, and not having any expert opinion, their disease gets untreated and further deterioration leads to irreversible states which immensely hampers the overall growth and development of the human mankind. Moreover, in remote villages no such expert persons are available who are capable of observing the symptoms accurately. An online secured transmission technique is needed for transmitting various clinical information to various physicians for their expert opinion, which emerges as a positive impulse towards socio-economic development of the country. Growth of Internet technologies have emerged to be as the key factor in the telehealth community (WHO 1998; Dey 2021). TMIS is very much convenient in the disease diagnosis through expert opinion, further treatment procedures, and exchanging the medical information for the research purposes, etc. However, the distance problem and the travelling cost may be minimized by the help of TMIS especially in this COVID era. Patients can avail appropriate medical diagnosis and treatments remotely from their homes or quarantines (Dey 2021; Chaudhry et al.

✉ Joydeep Dey
joydeepmcabu@gmail.com

¹ Department of Computer Science, M.U.C. Women's College, Burdwan, West Bengal, India

² Department of Computer Science and Electronics, Ramakrishna Mission Vidyamandira, Belur, West Bengal, India

³ Department of Computer Science, The University of Burdwan, Burdwan, West Bengal, India

⁴ AMRI Hospital, Salt Lake, Kolkata, India

2015). Empirical judgments are obtained from the experienced cardiologists, doctors, general physicians, cardiac surgeons, etc. to cure the patients soon and within the cost limits. Technological up gradation have filled the vacuum of non existence of the physicians especially in the remote areas. TMIS confiscates the said vacuum to an exemplary level and most appropriate in serving the patients during this global pandemic. Data security and privacy are the key issues to be addressed before communicating patients' data to the physicians. Apart from that there have been significant more issues that were raised in the Telecare Medical Information System of COVID-19. Capturing the signals in the middle paths by the intruders may force the patients' treatments in wrong guidance. In the period of corona virus, patients are more suggested to avail the remote telemedicine services due to lockdown and quarantine restrictions. Fraudsters are clever enough to decode the signals and reports when they are transported in the public medium (Kahate 2010). During this pandemic, the number of medical digital transactions had abruptly increased (Nan et al. 2021; Farr et al. 2021; Sageena et al. 2021). The key problem in this regard is the usage of same session keys for various transactions. Different session keys for different transaction sessions could defend the Man-In-The-Middle attacks in a convenient way (Dey et al. 2021a). In most of the COVID-19 telecare systems, another problem is the user authentication scheme. The authenticity of the users must be verified through a strong authentication protocol. Also it destroys the integrity of the Telecare Medical Systems (TMIS) during the COVID period (Bokolo 2021). Moreover, patients must have a control over the decryption phase (Sarkar et al. 2019b). That means they are to be given more power to control the system of genuine decryption.

Electro Cardio Gram (ECG) is used to represent the electrical activities of the heart muscle with respect to time domain in terms of milivolts (mV). Cardiac muscle contraction takes place with the event of electrical depolarization of the muscle cells present. ECG is the sum of this electrical activity when recorded for stipulated time slot. Analyzing the characteristics of ECG (Elham et al. 2011) signals leads to proper diagnosis and treatment for different types of cardiovascular diseases (CVDs) (Gopisetty 2017). The foremost organ that propels the survival of the human body is heart. Any malfunctioning that takes place within the cardiovascular region must be diagnosed immediately followed by exact line of positive treatments. Heart rate may be defined as the number of ECG cycles per minute. Cardiac arrhythmia is a severe condition with irregular heartbeats, either of too fast or too slow. The usual symptoms that are being observed while cardiac arrhythmia are palpitations or feeling like a pause in between two successive heartbeats with shortness of breath or mild or severe chest pain. Cardiac arrhythmia can aptly be diagnosed with the ECG signals which

comprises of P, Q, R, S, and T standard waves signals used in depolarization and repolarization of heart. Apart from these, there exists five another inter-wave timings known as PR, PR segment, QRS, QT, ST segment intervals. Details are shown in the following Fig. 1.

Metaheuristic approach in cryptography (Yang 2014) is a fresh accumulation concept. This approach may be embedded into the wide field of cryptography. Search exploration and exploitation are the two inevitable components of any metaheuristic algorithm. To explore the search space with global angle is the exploration. On the contrary, squeezing the search space into local area is the exploitation. Salp swarm (Mirjali et al. 2017) is a nature inspired metaheuristic algorithm based on exploration and exploitation. Balancing the exploration and exploitation variables is the prime objective of this algorithm. The proposed methodology focuses on dynamic key generation. High robustness ensures better non-distortion ability by the intruders. Stochastic algorithms are basically of two types heuristic and metaheuristic. Heuristic optimization techniques deal with the trial methods on several attempts until the goal state is not reached, within the local search space. On the other hand, metaheuristic means meta-data about the optimization technique. Randomization is the added feature in such techniques, so that all attempts give different set of solutions. It provides a scope to search on the global space (Mirjali et al. 2017). The overall architecture of Telecare Medical Information System has been represented in the following Fig. 2.

In the above stated Fig. 2, the existing architecture of Telecare Medical Information System (TMIS) has been represented. The services of TMIS are only possible through Internet. At the patient's end, their clinical signals are captured and are digitally transmitted into the Internet based public networks. On the reverse end, physician can be able to retrieve those data. Using the digital receiver system, the received data can be restored into its original format. Since,

Fig. 1 Components of an ECG curve

Fig. 2 Architecture of existing TMIS

the transmission medium is open to all, so the patients' data privacy is under of attacks. Intruders will easily steal the data and manipulate to a wrong meaning. This is the biggest challenge in such TMIS. In such existing TMIS, absence of cryptographic mechanism has been observed (de Oliveira Andrade et al. 2021; Peden et al. 2020). There should be adequate number of session key for different online transactions. During this worldwide corona virus pandemic, the use of telemedicine transactions had abruptly increased when compared to pre-COVID-19 times (Bokolo Anthony Jnr 2020). In order to maintain a strong confidentiality on the patients' data, there should be a higher cryptographic system on the TMIS. The proposed metaheuristic algorithm based encryption can enrich the security parameters. Moreover, the above mentioned limitations of the existing TMIS have been addressed in this proposed methodology based on salp swarm. The session key pool will have adequate number of session keys in the proposed TMIS. Different mathematical experiments were performed on the proposed technique to have the efficacy.

There exist several advantages of implementation of metaheuristic algorithms in cryptography. Firstly, it guarantees to generate efficient solution rather than global solution (Garg 2009). Secondly, more robustness in the secret key can be obtained through metaheuristic methods. Thirdly, the rate of convergence is higher than other algorithms in cryptography (Samanta and Chakraborty 2011; Manda et al. 2012). Fourthly, the fitness of each of the participating objects are evaluated at every iteration that helps to have more refined solution (Gomes de Freitas et al. 2010; Khajehzadeh 2011; Segura et al. 2017). Fifthly, secret keys can be derived using such metaheuristic algorithms (Sarkar et al. 2021). Despite of multiple advantages, there are some disadvantages of

Table 1 Some pros and cons of TMIS

PROS	Global treatment facilitation Expert medical opinions Avoiding noscomial infections Reduced treatment costs and time managements
CONS	Communication improvement Patient's data authentication control Assurance of data Integrity Data non-repudiation Very sensitive information access control Availability of information Large volume of data transmission

metaheuristic approach on cryptographic engineering. The proof of optimum solution cannot be guaranteed. The optimization control is fully dependent on the exploration and exploitation variables used in the problems (Parejo et al. 2012; Talbi 2002). Repeated same set of solution may not be generated with the same initial criteria. The global searching space gets expanded in this approach (Cowling et al. 2002).

The intellectual property of the swarm population (Mirjalei et al. 2017) embedded with the cryptographic algorithm is the key idea behind our proposed technology. Following Table 1 illustrates some of the pros and cons of the TMIS.

The manuscript has been organized in the following order. "Introduction" has the introduction parts. The related papers were surveyed and presented in the "Related works". Different types of challenges in the Telecare Medical Information System (TMIS) were cited in the "Challenges in TMIS". Solution domain has been mentioned in the "Solution domain". The proposed technique has been stated in the "Proposed technique". The proposed work flow diagram has been represented in the "Proposed work flow diagram". The novelties of the proposed technique have been given in the "Novelties of the proposed technique". "Results sections" contains the results. Analysis on comparison has been represented in the "Analysis on comparison". Gap analysis had been presented in the "Gap analysis". Conclusions, limitations and future scope of works were cited in "Conclusions, limitations and future scope". At the end acknowledgement, research funds, ethical statements, and references were added.

2 Related works

The cameo of novel coronal virus has significantly challenged the entire medical sciences throughout the world. Das et al. (2020) have proposed a deep learning Convolutional Neural Network (CNN) model. It is capable to detecting COVID-19 positive Chest X-Rays (CXr) from the pool of

healthy patients. They had achieved higher accuracy in such COVID-19 detection scheme. Swapna et al. (2020) have reported for developing novel digital schemes by the help of mathematical and statistical theory based on pulmonary disease in this COVID-19. Apostolopoulos and Mpesiana (2020) had evaluated the performances of Convolutional Neural Network topologies which were recently used for medical image classifications in this COVID-19 context. Dey et al. (2021a) had worked on cryptographic engineering on COVID-19 telemedicine with heterogeneous cardiac files.

Literature survey reveals that myriad authentication protocols have been designed to impose data security on the Telecare Medicine Information System (TMIS). Password and chip based smart cards are the two parameters of the two factor authentication protocols and three factor authentication protocol comprises of password, chip based smart card and biometrics. Registration phase, Login and Authentication phase, and Password Validation are the three primary phases to ensure user and data authentication. Moreover, they are also prone to vulnerable attacks from the intruders. Recently, chaotic encryption technology adopting the biometrics, iris, images, signals have been proposed. Murillo-Escobar et al. (2015b) had proposed a novel and secured authentication system on thirty two bits embedded system. Cui (2010) had developed a double round fingerprint encryption. Initially, fractional fourier domain has been used to encrypt the fingerprint. The resultant would be next encrypted with the chaotic confusion matrix. Khan et al. (2007) had proposed an encryption system where the secret key has been generated by the biometric information, and the same biometric can be used as initial condition of chaotic system. For every transaction, they had changed the biometric image to diffuse the intruding attacks. Awasthi and Srivastava (2013) had designed a pre-computing system to have secure authentication in the telemedicine. Their technique had lower time complexity. Murillo-Escobar et al. (2014) had developed 128 bits secret key on chaotic sequence. Key space analysis was done effectively to counter attack the intruding. Thus, it can be implemented in real applications. Patidar et al. (2009) had presented an encryption technique based on substitution and diffusion method. Their technique was fast and more secured one. Yan et al. (2013) had presented an encryption method on telecare medical information system. Their technique can easily withstand the Denial – of – Services attacks in the transmission paths. Lu et al. (2015) had developed an encryption method to withstand the secret key security issues and invalid users impersonations. Their technique was based on chaotic maps and smart cards which could be fruitful in telemedical services. Das and Goswami (2013) had designed an authenticated encryption technique which ensures efficient secret key storage and resistance against the MITM attacks. Chen et al. (2012) had suggested that strong

authentication method is recommended between the server and the remote users in the telecare systems. Their authentication method was more secured and robust in nature. Jiang et al. (2013) had proposed a biometric based remote authentication method to increase the users' security in telehealth. Their method had incurred less computing costs with respect to other methods. Lin et al. (2014) had proposed a dynamic ID authentication protocol that may be used in mobile computing. Their technique had outperformed earlier works and raised the security parameters. Through this, the number of concurrent users can be increased. Hao et al. (2013) had proposed another chaos oriented encryption. Their method was more suitable for telehealth services.

Chaotic encryption using Elliptic Curve Cryptography (Chaudhry et al. 2015), Chebyshev Chaotic Mapping (Parejo et al. 2012; Lu et al. 2015; Hao et al. 2013; Wang et al. 2015; Jiang et al. 2014; Lee and Hsu 2013), and Chaotic based Hash Function (Das and Goswami 2014) are the contemporary resistant techniques to such vulnerable attacks on the data. Specialists have proposed encryption calculations dependent on tumult for telemedicine network. Murillo-Escobar et al. (2017) have proposed a tumultuous capacity put together encryption with respect to the ECG/EEG signals in 2017. They have proposed a framework on the chaotic guide based encryption. In spite of the fact that they have attempted to force encryption hardness utilizing dissemination of disorganized framework, still the mistake of as far as Man-In-The-Middle (MITM) assaults has not been tended to appropriately. Here, the clinical ECG/BP/EEG signals of the patients that could be caught by the gatecrashers for phony or conflicting purposes. Made sure about online transmission of the private patients' information/signals should be managed information safeguarding sees. Usage of their proposed strategy has not been suitably clarified on the genuine application frameworks. Also, live detecting of the patients' signs and information pressure conduct was absent in their work. Raeiat-ibanadkooki et al. (2016) in the year of 2016 have proposed a technique to pack and scramble the ECG with wavelet change and tumult based Huffman code. The principle objective is to crush and scramble the ECG without loss of any information. Lin (2016) had proposed a disordered visual cryptosystem with a view towards observational mode deterioration and calculated guides for the EEG signal. Lin et al. (2014) had proposed mayhem put together encryption strategy with respect to calculated guide to scramble the ECG signals. Notwithstanding, the security investigation was passed up a great opportunity. Atal and Singh (2020) had proposed a new embedding technique on the ECG signals. The ECG signals were compressed by Dictionary Matrix Generation algorithm, followed by covering image. Their technique had reduced data loss and time complexity. However, a thorough investigation was more need in that technique from the security perspectives.

Telecare Diagnosis Systems have been arisen as a treatment instrument in online wellbeing network. Scientists are investing their best amounts of energy to give more adaptable framework to the general public. Mulyad and Nelmiawati (2019) have proposed how to improve the exactness of a 12-lead ECG utilizing waveform segmentation of ECG charts. Liaqat et al. (2016) have planned a structure to build up connections between different cardiovascular patients' credits utilizing unaided learning procedures. They have applied the K-mean (quick) calculation alongside connection and likeness of information module to determine the shrouded connections among various patients' ascribes. Capua et al. (2010) have proposed a method to screen and survey the ECG signals continuously. ECG signals are detected through sensor and prepared by an individual computerized collaborator (PDA). The PDA may identify and analyze the ECG signals, and call the crisis faculty in the event of anomalies recognized. Patients can likewise envision the ECG clinical signs inside the PDA interface. Borghetti et al. (2013) have built up a sensor based glove to quantify hand finger flexion for recovery. It comprises of a glove and a bunch of sensors set at the constant securing unit with proper setup, which thusly offer input to restoration unit utilizing patients' fingers positions. Karpagachelvi et al. (2010) have proposed how to extricate the fundamental highlights from the ECG signals. Looking through the particular focal points to extrapolate timing and greatness estimations in the ECG diagrams is finished. Here, the regular highlights are associated with pinnacles and timings of P, QRS and T waves parts in ECG. Mahmoodabadi et al. (2006) have proposed to distinguish and recognize the QRS complex and the heights and dejections of the P and T waves on the MIT-BIH signal information base dependent on multi goal. Daubechies D4 and D6 wavelet changes with a triumph pace of 98%. Fatemian and Hatzinakos (2009) have built up a quadratic Spline wavelet based system. Their goal was to investigation of single lead ECGs for human ID naturally. Purposes of maxima, minima and zero intersection esteems in the discrete wavelet coefficient recreation of the ECG signals at various scales are gotten prior to recognizing the QRS, P and T fiducial focuses. This fiducial methodology has discovered positive acknowledgment of 99.61% utilizing the clinical signs of the MIT-BIH information base. Ye et al. (2010) have proposed a fiducial free methodology with a positive acknowledgment achievement pace of almost 99.6%. Applying the Daubechies wavelet of request 8, the wavelet coefficients were extricated. The Independent Component Analysis (ICA) has been used to acquire the free segments by sifting the factual autonomous arbitrary factors. At that point the PCA have been utilized to limit the elements of the extricated highlight of ECG. Sarkar et al. (2019a) had shown an intelligence technique to encrypt the

cardiac related data. They have used multiple recipients for sharing the ECG files.

3 Challenges in TMIS

Made sure about the online transmission of clinical signals between the patients and doctors is the main point of contention particularly when the vast majority of the exchanges are done online in this COVID-19 period. Interlopers are destined to sniff the patients' private data, and they do mutilate or control with these. To safeguard the private boundaries of the patients, there necessities to execute a high made sure about online exchange framework dependent on Telecare Medical Information System (TMIS). Infection finding is the initial phase in treating any type of illness. Patients desire to hear an accurate and solid point of view from the specialized doctors. In fact, it is more necessary to have these services from their quarantines / homes in order to reduce the COVID-19 transmission. The current TMIS has a few bad marks with respect to the earlier works done. Some of them are enrolled beneath.

- Existing transmission strategy of TMIS may treat the chance of willing divulgence of patients' clinical reports and clinical signs for such a negative works.
- Lack of data authentication and confidentiality checking mechanisms exist in the TMIS. Hence, the data integrity of patient cannot be achieved in such advanced Telecare Medical Information System.
- Excessive use of online medical transactions due to COVID-19 lockdown bindings.
- Spillage of such significant clinical signs may prompt the abuse and phony mediclaim strategy repayment issue.
- Indeed, even the patients have no component to oppose the exposure of her/his classified clinical information on more extensive scale.
- Same session key used for multiple transactions in the TMIS. Contemporary works on COVID-19 have not proposed multiple session keys for online medical transactions.

4 Solution domain

The foible of existing TMIS transmission systems discussed in the above section may be eliminated through proposed technique. In this proposed technique, a salp swarm based metaheuristic approach has been proposed for generation of robust session keys. These keys could be efficiently be used for different concurrent transaction. It would be very much effective when the patients are not able to attend the

hospitals physically due to the fear of getting COVID-19 attack. COPD patients have huge chances of COVID-19 attacks if underwent to hospitals physically. The patients' clinical signals are highly confidential and needed to be kept hidden. To leap towards data secrecy, the proposed technique plays a pivotal role at the secured online transmission of clinical signals. Nature inspired Salp swarm optimization algorithm (Yang 2014) is used for secret session key generation. Salp swarm based optimization guided by the exploration and exploitation variables. The best fitted salp is assigned as the leader, and the rest of the swarm are followers. In the context of optimization, the leader may always not be least deviated from the food source in terms of the path. The fittest leader will serve as a session key for this cryptographic approach. The key pool will treat individual keys for different medical transactions.

This proposed technique can be attached with existing COVID-19 TMIS as a highly secured online medical information transmission module.

5 Proposed technique

In the field of cryptography, metaheuristic algorithms can be molded to generate a robust session key. The scenario developed as a result of COVID-19, had emerged the more needs of telehealth. The key idea is to encrypt the ECG signals before transmission. Thus the cryptogram designed would be transmitted to the network to other doctors. Nature inspired biological simulations of species may create an extensive set of keys to masquerade the ECG components (Murillo-Escobar et al. 2015a). The behavior of salp swarm manifests our proposed frame of work. The elegance of nature is that every species hunt for their closest food source to survive. The proposed technique simulates the swarm behavior of the salps to have the session key. Improving the solution from each step by keeping a track on the true randomness of the leader's positions is desirable. Salps belong to the Salpidae family which resemble like jelly fish. Architecture of the proposed COVID-19 TMIS has been shown in the following Fig. 3.

5.1 Proposed salp swarm algorithm guided fittest session key generation

To formulate mathematically, salp chain is divided to two groups like leader and the followers. The first salp is termed

Fig. 3 Architecture of proposed COVID-19 TMIS

as leader who guides the entire swarm of salps, whom the rest follow, termed as followers (Mirjali et al. 2017). The vector position of salp is defined in n -dimensional search space where n denotes number of variable of a domain, which is stored in double-dimensional matrix. Three dimensional co-ordinates are initialized randomly confined in the n dimensional space. Similarly, the food source called F is the search space is the swarm's destination. Food colony is also created as a double dimensional matrix comprising of the co-ordinates system. Each salp is designated with an additional weighted vector of 128 bits long. The elegance of this vector is to find the fitness level suitable for the safe encryption. A message digest would be formed using the MD5 function. This receives the concatenated co-ordinates of each salps to determine its weighted vector. MD5 function returns a true random string. Moreover, among the population salp set, fittest weighted vector is adequately enriched to select the session key for encrypting the ECG signals. The complete process of fittest key generation is illustrated in following Algorithm 1. Food source fill process has been discussed in the Algorithm 2.

Algorithm 1: Fittest Session Key Generation

Input(s): PS: Population Size of Salp, lbx, ubx, lby, uby, lbz, ubz: Lower & Upper limit of salps, LBx, UBx, LBy, UBy, LBz, UBz: Lower & Upper limit of salps,
Output(s): Session Key
/ Weighted Salp Initialization */*
1: For I = 0 to (PS - 1) do
2: $Salp[I][0] \leftarrow RND(lbx, ubx)$
3: $Salp[I][1] \leftarrow RND(lby, uby)$
4: $Salp[I][2] \leftarrow RND(lbz, ubz)$
5: $Salp[I][3 \dots 130] \leftarrow \text{CodeHash}(Salp[I][0] + ', ' + Salp[I][1] + ', ' + Salp[I][2])$
6: $i = i + 1$
7: End for
/ Food Matrix SpaceCreation */*
8: FoodSM[r][3] $\leftarrow$ Call *Food_Matrix_Fill* (LBx, UBx, LBy, UBy, LBz, UBz)
9: While (! Max_Iterations)
10: For I = 0 to (PS - 1) do
11: $Rng1 = \{ (2 * \exp e^{\frac{(-4 * ip)}{(im)^2}}) \}$
12: If (Rnd(R1, R2) $\geq$ 0) Then
13: $Salp[0][0 \dots 2] = AVG(FoodSM) + [\{ UB_n - LB_n \} * RND[0,1] + LB_n] * RND[0,1]$
14: Else
15: $Salp[I][0 \dots 2] = AVG(FoodSM) - [\{ UB_n - LB_n \} * RND[0,1] + LB_n] * RND[0,1]$
16: End if
17: $Salp[I][0 \dots 2] = \frac{1}{2} * (Salp[I][0 \dots 2] - Salp[I - 1][0 \dots 2])$
18: Fit $\leftarrow$ Fitness(Salp[I][3 ... 130])
19: If (Fit) Then
20: Temp $\leftarrow$ IncreaseSort (Salps[PS][0 ... 130])
21: Else
22: Bit_Reshuffle(Salp[I][3 ... 130])
23: Fitness(Salp[I][3 ... 130])
24: Temp $\leftarrow$ Sort (Salps[PS][0 ... 130])
25: End if
26: End for
26: End while

In the above stated code of salp swarm, there lies an immense significance of the exploration and exploitation concepts. Exploration covers the search of food source in larger coordinates space. It prevents the solution stagnation. The leader salp explores the food source and update their position through the above algorithm steps 12–15 in each epochs. While the follower salps update their positions through step number 16. In step number 11, a variable Rng1 has been calculated to balance these two phenomenons of exploration and exploitation (Abramowitz and Stegun 1965). It is extremely helpful to diffuse the salp positions from the external intruders. Since the coordinates of the food source were kept hidden to the intruders, so they are unable to decode the proposed session key. Moreover by shuffling the positions of the leader salps in the key pool provides more robustness in the fittest secret key. Thus, the patients' data cannot be distorted easily by the

intruding, which is an essential criterion in the Telecare Medical Information System (TMIS) of Post-COVID-19.

5.1.1 Proposed food matrix fill algorithm

This algorithm fills the food matrix space in three dimensional size. The dimensions of the food matrix has been presumed beforehand.

Algorithm 2: Food Matrix Space Creation

Input(s): Food Colony nos. : FC, Limits of axes: LBx, UBx, LBy, UBy, LBz, UBz

Output(s): Food Matrix : FoodSM[DS][3]
1: For I = 0 to FC - 1 do
2: $FoodSM[I][0] \leftarrow RND(LBx, UBx)$
3: $FoodSM[I][1] \leftarrow RND(LBy, UBy)$
4: $FoodSM[I][2] \leftarrow RND(LBz, UBz)$
5: $I = I + 1$
6: End For

5.2 Proposed fitness test algorithm

The proposed technique generates the optimal session key by testing the fitness level of the salps. The weighted vector of 128 bits long would be statistically proved its randomness. Furthermore, in case of failure to pass the proposed fitness test function, the weighted vector of the leader salp will be dragged into bit restructuring process to achieve its fitness. In this process, randomly certain number of bit positions is identified from the weighted vector dissatisfying the proposed fitness function. The corresponding bits are get flipped, and re-assessed the fitness values seeking the threshold value. The 128 bit salp based session key is statistically fittest enough to reduce the chances to intercept the ECG signals by eavesdroppers. The pseudo code used in the TMIS to test the fitness of leader salp is given below. Standard `erfc()` function have been accessed in the following proposed Algorithm 3 (Abualigah et al. 2020).

Algorithm 3: Statistical Fitness(KEYST[128])Test

Input(s): Key Value: KEYST[128]

Output(s): True (1) or False (0)

```

1: Assign One, VAL, x, y  $\leftarrow$  0.0;
2: Assign r, j, i  $\leftarrow$  0
3: While [ i < 128 ] do
4:   If ( KEYST[i] == 1 )
5:     One  $\leftarrow$  One + 1
6:   End if
7:   VAL  $\leftarrow$  (One * 1.0) / 128
8:   i  $\leftarrow$  i + 1
9: End while
10: For j = 0 to 127 do
11:   If ( KEYST[j]  $\neq$  (KEYST[j + 1])) then
12:     j  $\leftarrow$  j + 1
13:   End if
14: End For
15: x = ABS(r - (2 * 128 * VAL * (1 - VAL)))
16: y = 2 * (SQRT( 2.0 * 128) * VAL * (1 - VAL))
17: p - value  $\leftarrow$  Call erfc( $\frac{x}{y}$ )
18: If (p - value  $\geq$  0.05 ) then
19:   Return (1)
20: Else
21:   Return (0)
22: End if

```

In the above stated algorithm, we have evaluated the statistical fitness of each salps. The weight vectors of the salps were tested through the above codes. If any salp cannot qualify that fitness test, then randomly certain number of bits was altered to generate its higher degree of fitness. This fitness test provides robustness in the proposed session keys.

5.3 Proposed encryption algorithm

A block-wise AES-128 encryption is performed on plain clinical signal. Here, the statistical test qualified Salp swarm guided fittest 128 bit long weighted vector act as a key for the AES-128 algorithm. In a classical AES algorithm (Karthigaikumar et al. 2015), a randomly chosen 128 bit AES key may not qualified for all statistical tests. So, generation of robust key for AES is always an issue. The strength of the encryption algorithm entirely depends on the randomness of the key sequence. The question is how random the chosen random key is? To generate a truly random key sequence our proposed technique have used salp swarm guided metaheuristic search and statistical randomness test as a fitness function of this search algorithm. In this encryption algorithm a plain signal of block size 16 is chosen for performing 10 rounds encryption. At each round *SubBytes()*, *ShiftRows()* and *MixColumns()* operations are performed. Finally, an encrypted signal of block size 16 is generated at the end of the 10 rounds. Algorithm 4 illustrates the encryption procedure.

Algorithm 4: Cipher(InBlock[16], OutBlock[16], w[0 ... 43])

Input(s): Plain Signal of Block size 16

Output(s): Encrypted Signal of Block size 16

```

1: BlockToState (InBlock, S)
2: S  $\leftarrow$  AddRoundKey (S, w[0 ... 3])
3: For round 1 to 10 do
4:   S  $\leftarrow$  SubBytes (S)
5:   S  $\leftarrow$  ShiftRows (S)
6:   If (round  $\neq$  0 )then
7:     S  $\leftarrow$  MixColumns (S)
8:   End if
9:   S  $\leftarrow$  AddRoundKey (S, w[4  $\times$  round, 4  $\times$  round+3])
10: End for
11: StateToBlock (S, OutBlock);

```

5.3.1 Key expansion algorithm

A key expansion algorithm is performed on salp swarm generated 128 bit fittest key to generate 128 bit for each round of the AES-128 encryption algorithm. Algorithm 5 shows this entire key expansion process.

Fig. 4 Schematic flow diagram of proposed COVID-19 TMIS

Algorithm 5: KeyExpansion([key₀ to key₁₅], [w₀ to w₄₃])

Input(s): Salp Swarm Generated 128 bits fittest key

Output(s): 128 bit key for next round

```

1: For i = 0 to 3 do
2:    $w_i \leftarrow key_{4i} + key_{4i+1} + key_{4i+2} + key_{4i+3}$ 
3: End for
4: For i = 4 to 43 do
5:   If (i mod 4  $\neq$  0) then
6:      $w_i \leftarrow w_{i-1} + w_{i-4}$ 
7:   Else
8:      $t \leftarrow SubWord(RotWord(w_{i-1})) \oplus RCon/4$ 
9:      $w_i \leftarrow t + w_{i-4}$ 
10:   End if
11: End for

```

Using the modified salp swarm algorithm, fittest weighted vector is selected to encrypt the ECG signals (Sarkar et al. 2020). Robustness of the key is identified on higher degree. The proposed model can anticipate how to resist the sniffing. TMIS are prone to vulnerable attacks. However, the proposed technique encounters such vulnerable attacks, which has been discussed in the later section.

Fig. 5 ECG WAVEFORMS of 10 s interval

6 Proposed work flow diagram

The following Fig. 4 shows the schematic diagram of proposed technique in TMIS, which may be used in this COVID-19 crisis. It is a secured transmission technique that may cope up the needs of telemedicine at the hours of COVID-19.

7 Novelties of the proposed technique

In this sub-section, we have presented our novelties in this proposed technique. The following are the novelties of this proposed Post-COVID-19 TMIS, which are presented in stage-wise manner.

- Non-invasive and non-critical patients can remotely be treated by the proposed COVID-19 TMIS.
- Salp swarm based session key has been generated for better encryption.
- Multiple session keys for concurrent session of the TMIS have been proposed.
- Modified AES has been implemented with the proposed metaheuristic session key of 128 bits.
- Fitness function for the session keys has been proposed.
- Efficacy achieved in the experimental sections when compared with others.
- Telecare Medical Information System to curtail the Post-COVID-19 transmission through remote health services.
- Online secured transmission of patients' clinical data in a very secured manner.

Fig. 6 EEG during mental arithmetic task

Fig. 7 UCD sleep apnea database

8 Results sections

The proposed algorithm has been implemented in MATLAB v7.6 (R2008a) with Intel i7:2.6 GHz processor, 8 GB RAM, and Windows 10: 64-bits. A comprehensive and needful security views have been focused to affect the acquaintance security and robustness issues. Precision of 10^{-15} decimal have been used in arithmetic operations according to authenticated Institute of Electrical and Electronics Engineers (IEEE) Standard 754. Cryptogram should possess random properties to masquerade the ECG of the patients. In addition the key generated should also resist cryptanalyst attacks like exhaustive key attacks, geometrical attacks, statistical attacks, chosen plain signal attack, differential attacks, etc.

ECG signals were accessed from PhysioBank ATM for BIMDC Congestive Heart Failure Database (chfdb) with output length duration of 10 s (Physionet.org 2016). Figure 5 shows a snapshots derived from the said database. Furthermore, Figs. 6 and 7 show EEG During Mental Arithmetic Task and UCD Sleep Apnea Database Waveforms of all signals with 10 s output duration respectively (Murillo-Escobar et al. 2017). The proposed technique generates the session key and encrypt the ECG signal mentioned in the following Fig. 5 with the AES encryption algorithm. Using the metaheuristic approach of salp swarm behavior, fittest session key has been derived. This resultant key would be used to encrypt the clinical signal, and the ciphered signal may be transmitted by the cardiologists / doctors. The proposed technique protects the confidential matters related to the patients' diseases / reports. Thus a humongous scope of better treatment is open in the face of Post-COVID-19 pandemic.

Moreover, the following Table 2 displays top ten outputs of 1035 total rows of salp leaders' co-ordinates and corresponding digest as their respective weighted vectors. The weight vector of fittest salp is considered as the session key. Furthermore, it is used to encrypt the ECG signals in TMIS. Robustness of the proposed technique can be achieved by the inability to detect by the intruders. TMIS embedded with optimization technique has been adopted at this paper. With a flip of bit in the leader salps' co-ordinate, there will be significant

changes in the key generation. Thus, it would be really impossible to detect / predict the session key by the intruders.

8.1 Statistical fitness test analysis

The above stated session keys as given in Table 2 were fed into the proposed fitness function (Algorithm 3). The following Table 3 shows the summary this fitness test evaluation. Thus the robustness of the proposed session key may be established through this.

From the above Table 3, it can be noted that the keys as given in Table 2 have successfully passed the proposed fitness test here. Thus, such robust session keys are useful in transmitting patients' medical data during this pathetic Post-COVID-19 period.

8.2 Information entropy analysis

The entropy of a clinical signal is an index of its data content. It is measured in terms of bits per character in a signal. If a character has a very chance of occurrence, then its data content is very less. Any document will carry in between 0 and 255 characters. Entropy value of such document will be in between 0 bit per character to 8 bits per character. 8 bits per character denotes equally spread data values. The plain

Table 3 Summary of the proposed fitness function

Key id	Session key sequence having p value larger than 0.05	Proportion %	Outcome
1	885	0.885	Passed fitness
2	917	0.917	Passed fitness
3	881	0.881	Passed fitness
4	954	0.954	Passed fitness
5	882	0.882	Passed fitness
6	949	0.949	Passed fitness
7	971	0.971	Passed fitness
8	892	0.892	Passed fitness
9	902	0.902	Passed fitness
10	924	0.924	Passed fitness

Table 2 Snapshot of top ten weighted vectors of leader salp

Key id	Leader Salps' coordinates	Weighted vector of leader
1	137,3118,42	669b3c9f47954aa414d05e94a516d1a2
2	1694,489,786	d3b5e5ead2f87c1c56ca7dbe7ab13caa
3	588,74,692	10a1559e91c2a4309c51c84ade88b5c2
4	874,512,120	ee306e0985dd991b78a39fd361622ae5
5	741,98,236	25d16ae06fc5c548f25f3491d25bdc82
6	518,981,1315	0e1a33eScbcd45d29d74036c0a4d816
7	77,547,801	cd43eafab0c1a42c1e378ff020183cd0
8	690,274,16	bcd1bf208d9c4cb40c1af60d1dfd09e6
9	876,784,141	dad608555d0bd0fa2bb760b83775cb64
10	225,1102,2004	af7ec4ca9e217be0a7e94db7690a54be

Table 4 Entropy values after encryption

Key id	Entropy of plain ECG signal	Entropy post encryption	Maximum entropy
1	7.69	7.96	8.00
2	7.69	7.90	8.00
3	7.69	7.92	8.00
4	7.69	7.94	8.00
5	7.69	7.91	8.00
6	7.69	7.93	8.00
7	7.69	7.98	8.00
8	7.69	7.87	8.00
9	7.69	7.92	8.00
10	7.69	7.94	8.00

clinical signal given at Fig. 5 is encrypted using proposed technique. Following Table 4 contains a comparison between the entropy of plain clinical signal and entropy after proposed encryption. The acceptance of the proposed technique can be revealed from the following Table 4 with favorable results.

8.3 Histogram analysis

The identification of ECG waveforms and their characteristic features is an important task for the diagnosis of diseases. In this proposed work, histograms are a graphical demonstration of numerical data of equal size and it is used as an estimator of ECG signal. Histograms are basically generated by measuring the variations of the orientations among these sample values in some directions. A peak is a bar that is taller than the neighboring bars. If two or more adjacent bars have the same height but are taller than the neighboring bars, they form a single peak or plateau. A gap is a class or classes having frequency zero, but with non-zero frequency classes on both sides. Extreme values are data values which are separated from other data values by a gap at least two classes wide (Fig. 8).

8.4 Floating frequency analysis

Floating frequency of a signal is a characteristic of its local data content at sample points inside the signal. It specifies the number of different characters present at any given 64 character long fragment of the signal. The function considers sequences of signal characters in the active window of 64 characters long. It also counts how many different characters are located at the current window. After that, the window is moved by one character to the right and the same calculation is repeated again and again. This procedure summarizes the signal in which it identifies the positions with high and low data density. A signal of length N bytes ($N > 64$ bytes) has $(N - 63)$ such index numbers in its characteristics (Fig. 9).

8.5 Autocorrelation analysis

Autocorrelation is an empirical test of independence which checks the correlations between the succeeding outcomes of the encryption and /or between the binary data streams 1 and an alternative version of 1s that can be replaced by $t1$ positions. Consider $t1$ be a positive number that lies in between $[1, ((n/2))]$ (Fig. 10).

8.6 Graphical efficacy

Session key generated at the above Table 3 have been indulged to generate the proposed cryptograms. The following Figs. 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39 and 40 figure out the goodness of the proposed technique by highlighting the comparison in terms of histogram, floating frequency, and autocorrelation graphs with their corresponding session key serially.

The histograms of Figs. 11, 14, 17, 20, 23, 26, 29, 32, 35, and 38, uniformity in the histogram charts were found. Thus, it is a good sign of proposed encryption. The floating frequency figures as mentioned in Figs. 12, 15, 18, 21, 24, 27, 30, 33, 36, and 39 had shown well distributed characters in the proposed cipher texts by using different keys. In the above autocorrelation Figs. 13, 16, 19, 22, 25, 28, 31, 34, 37, and 40, it has been observed that no fixed determining patterns

Fig. 8 Histogram of plain clinical signal at figure **Fig. 9** Floating frequency of plain clinical signal at Fig. 5

Fig. 10 Autocorrelation of plain clinical signal at Fig. 5

Fig. 11 Histogram of clinical signal at Fig. 5 with Key_ID=1

Fig. 12 Floating frequency of clinical signal at Fig. 5 with Key_ID=1

Fig. 13 Autocorrelation of clinical signal at Fig. 5 with Key_ID=1

Fig. 14 Histogram of clinical signal at Fig. 5 with Key_ID=2

Fig. 15 Floating frequency of clinical signal at Fig. 5 with Key_ID=2

Fig. 16 Autocorrelation of clinical signal at Fig. 5 with Key_ID=2

Fig. 17 Histogram of clinical signal at Fig. 5 with Key_ID=3

Fig. 21 Floating frequency of clinical signal at Fig. 5 with Key_ID=4

Fig. 18 Floating frequency of clinical signal at Fig. 5 with Key_ID=3

Fig. 22 Autocorrelation of clinical signal at Fig. 5 with Key_ID=4

Fig. 19 Autocorrelation of clinical signal at Fig. 5 with Key_ID=3

Fig. 23 Histogram of clinical signal at Fig. 5 with Key_ID=5

Fig. 20 Histogram of clinical signal at Fig. 5 with Key_ID=4

Fig. 24 Floating frequency of clinical signal at Fig. 5 with Key_ID=5

Fig. 25 Autocorrelation of clinical signal at Fig. 5 with Key_ID=5

Fig. 29 Histogram of clinical signal at Fig. 5 with Key_ID=7

Fig. 26 Histogram of clinical signal at Fig. 5 with Key_ID=6

Fig. 30 Floating frequency of clinical signal at Fig. 5 with Key_ID=7

Fig. 27 Floating frequency of clinical signal at Fig. 5 with Key_ID=6

Fig. 31 Autocorrelation of clinical signal at Fig. 5 with Key_ID=7

Fig. 28 Autocorrelation of clinical signal at Fig. 5 with Key_ID=6

Fig. 32 Histogram of clinical signal at Fig. 5 with Key_ID=8

Fig. 33 Floating frequency of clinical signal at Fig. 5 with Key_ID=8

Fig. 37 Autocorrelation of clinical signal at Fig. 5 with Key_ID=9

Fig. 34 Autocorrelation of clinical signal at Fig. 5 with Key_ID=8

Fig. 38 Histogram of clinical signal at Fig. 5 with Key_ID=10

Fig. 35 Histogram of clinical signal at Fig. 5 with Key_ID=9

Fig. 39 Floating frequency of clinical signal at Fig. 5 with Key_ID=10

Fig. 36 Floating frequency of clinical signal at Fig. 5 with Key_ID=9

Fig. 40 Autocorrelation of clinical signal at Fig. 5 with Key_ID=10

has been located in such graphs when plotted through different session key.

8.7 Analysis of quality metrics

The quality analysis on the encrypted ECG signal had been carried out in this section. It involves the mean-squared error (MSE), root mean-squared error (RMSE), peak signal-to-noise ratio (PSNR), and structural similarity index (SSIM) under our test. MSE may be computed as to measure the difference between the original signal X and encrypted signal E with length L using the following Eq. (1) (Khan and Shah 2014).

$$MSE = \frac{\sum_{i=1}^L (X_i - E_i)^2}{L} \quad (1)$$

Root mean-squared error (RMSE) (Willmott and Matsuura 2005) is the square root of the values observed in the above Eq. (1) of MSE.

$$RMSE = \sqrt{\frac{\sum_{i=1}^L (X_i - E_i)^2}{L}} \quad (2)$$

Higher MSE value is always desirable by the encryption algorithm. Peak Signal -to- Noise Ratio is the ratio between the maximum pixel values to the compressed image (Setiadi 2021; Liu and Zhai 2017), which is illustrated in the following Eq. (3).

$$PS = 10 \log_{10} \left(\frac{MAXPIXEL}{MSE} \right) \quad (3)$$

MAXPIXEL represents the maximum number of pixels present in the original signal, and MSE as computed from Eq. (2). Structural Similarity Index (SSIM) is a tool to measure the quality of the compressed image (Chen and Bovik 2011). It involves the mean, standard deviation, and cross correlation between the original image and the compressed image, as explained in the following Eq. (4).

$$SSIM(x, y) = \frac{(2\mu_x\mu_y + C_1) \times (2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1) \times (\sigma_x^2 + \sigma_y^2 + C_2)} \quad (4)$$

μ_x, μ_y are the mean of the original image and compressed image respectively, σ_x, σ_y are the variance of the original image and compressed image respectively and σ_{xy} is the

correlation between the original image and compressed image respectively (Chen and Bovik 2011), $C_1 = \{0.01 \times (2.256 - 1)\}$, and $C_2 = \{0.03 \times (2.256 - 1)\}$.

Percentage Root mean squared deviation (PRD) (Stangierski et al. 2019) is used to measure the distortion in the original ECG signal and derived ECG from database using the following Eq. (5).

$$PRD = (MSE)^{0.5} \times 100 \quad (5)$$

In the following Table 5, a comparison between the different clinical signals corresponding to the quality metrics as stated above has been briefly formatted.

The fitness of the individual salps has been tested in this proposed technique. In the next Table 6, RSME were calculated on different session key pool in brief.

From the above stated Table 6, we can say that the error ratio of the proposed fitness function (Algorithm 3) was extremely low which is more suitable in such cryptographic system.

8.8 Chosen plain signal attack

Cryptographic calculations are notable to the general population. The solitary concealed mystery is the key, through which encryption had been accomplished. Gatecrashers present quietly on the organization, will test a few arrangement of keys to unscramble the code text. In the TMIS, aggressors attempt to decode the ECG signal parts dependent on some heuristic keys. Length of the key size is proportionate to the intricacy to oppose against the picked plain sign assaults. It is a device to break picture encryption under disorderly succession (Murillo-Escobar et al. 2015). The proposed salp swarm based encryption algorithm is robust to such chosen plain signal attack. Session key that has been generated from the fittest leader salp after passing through fitness test. Even a one bit flip in the leader's coordinate will immensely modify the corresponding weight vector value on 128 bits. Similitude between the co-ordinates and corresponding hash value is ideally not feasible due to its randomness. This proves the resistant by the proposed technique against the chosen plain signal attack in the Post-COVID-19 Telecare Medical Information System (TMIS).

8.9 Noise attack

Changes looking like the communicated ECG signs may delude the cardiologist to analyze the infection. Signs are

Table 5 Quality matrix value

Sl no.	Data signal	Value of MSE	Value of PSNR	Value of SSIM
1	ECG Signal (Physionet.org 2016)	28,967.85	4.1	0.07
2	EEG Signal (Physionet.org 2016)	26,329.20	9.2	0.08
3	UCD ignal (Physionet.org 2016)	21,897.63	6.9	0.06

Table 6 RSME of session keys

Sl. no.	No. of session key	RSME	No. of keys failed	Error ratio
1	10	81.17	00	00
2	50	84.09	01	0.02
3	100	89.32	03	0.03
4	120	91.44	02	0.017
5	150	85.26	04	0.027

mutilated by the impact of commotion factor, named as clamor assault. The proposed procedure is impervious to the said assault in the accompanying manner. The ECG signal has been misshaped by *imnoise()* with commotion esteem 0 as salt and 1 as pepper. Three diverse commotion thickness cases are 0.017, 0.048, and 0.156 scaled at 2, 5, and 15% of clamor individually. In ideal circumstance, Mean-squared Error, MSE ought to be nil, anyway not reasonable that one. MSE between unique sign and unscrambled signal is 97.21, 420.17, and 1371.40 for 2, 5, and 15% of commotion individually in case of clinical ECG. Percentage Root-mean-square Difference for the clinical EEG signal has been obtained as 18,751.26, 26,821.12, and 47,821.02 at 2, 5, and 15% noise levels respectively. Following Tables 7, 8 and 9 given underneath contains the values for the clinical signals (Physionet.org 2016). Utilizing the clamor assault, the data sent from patients to cardiologists/doctors or the other way around, may lose. By raising the sampling frequency f_s , this expressed issue of lost sign might be tended to.

8.10 Brute-force attack

The large key space makes the brute force attack infeasible. In this attack, attacker tries to translate the cipher text into plain text using every possible key. The length of the session key proposed here is $L=128$. On average, half of all possible keys are enough for achieving success. Algorithms are known to all in most networking system but brute-force attack will impossible if the algorithm uses large key space. IBM Summit at Oak Ridge, USA, invented the fastest supercomputer in the world with 148.6 PFLOPS, i.e., means 148.6×10^{15} floating-point operations per second. Certainly, it can be considered that each trial may require 2000 FLOPS to undergo its operations. So number of trials complete per second is: 104.27×10^{62} . The number of second in a

Table 7 Effect of noise on ECG signal

Sl. no.	Variation in noise level	Noise density	MSE	PRD	RSME
1	NL=2%	0.016	97.21	18,751.26	9.859
2	NL=5%	0.046	420.17	26,821.12	20.498
3	NL=15%	0.162	1371.40	47,821.02	37.032

Table 8 Effect of noise on EEG signal

Sl. no.	Variation in noise level	Noise density	MSE	PRD	RSME
1	NL=2%	0.010	90.45	397.09	9.510
2	NL=5%	0.039	365.59	514.84	19.120
3	NL=15%	0.147	1295.62	865.62	35.994

Table 9 Effect of noise on UCD signal

Sl. no.	Variation in noise level	Noise density	MSE	PRD	RSME
1	NL=2%	0.021	94.51	91.26	9.721
2	NL=5%	0.048	501.29	149.95	22.389
3	NL=15%	0.187	1451.18	310.52	38.094

Table 10 Time required deciphering the session key

Length of session key	No. of possible combinations	Time needed to decipher (years)
128 bits	2^{128}	8.66×10^{52}

year are $365 * 24 * 60 * 60 = 3153600s$. Now from the above key space the formula for break the session key is $2^L / (104.27 * 10^{62} * 3153600) = T$. Here, T denotes number of years. So if L increases then Y increases ($L \propto T$) thus for large key length it is difficult to break the key. A cipher text with such a long key space is sufficient for reliable practical use. This proves that a key with large enough is sufficient enough to overcome the brute force attack. Consequently, this proposed technique will be resolved to be a strong cryptographic system in obvious future too (Table 10).

Thus, it may be stated that the proposed set of session keys are robust enough while performing the cryptographic functions in the Post-COVID-19 TMIS.

8.11 Occlusion attack

In Post-COVID-19 TMIS signal transmission, it evident that it will lose information to certain extent. The recovery of the plain signal from the cipher text are evaluated through occlusion attack. Mean Squared Error (MSE) has been considered

Table 11 Occlusion attack values estimation

Sl. no.	No. of ECG signal elements	MSE for 2%	MSE for 5%	MSE for 15%
1	30	129.63	268.16	1140.12
2	100	467.32	751.90	2835.06
3	150	647.00	1421.36	4587.05

here as its measure. The resilience level of such ECG signal has been assessed in the proposed procedure against impediment assault. Signs lost with higher than 5% isn't appropriate for contemplations. ECG sign of Fig. 5 have 850 sign components somewhere in the range of zero and one. Arbitrarily, 30, 100, and 150 components were chosen and characterized as zero. The MSE of recuperated ECG signals considering 30 random sample elements is 129.63 for 2% commotion, 268.16 for 5% clamor, and 1140.12 for 15% commotion (Table 11).

8.12 Cryptographic time

The proposed technique can be used to transmit patients' data to the cardiologists or physicians in this corona virus pandemic. For any such telecare system, cryptographic time is another key aspect. The following Table 12 contains the cryptographic timings obtained during our testing phase.

Table 12 Proposed cryptographic time

Sl. no.	Data signal	No. of data elements	Encryption time (in s)	Decryption time (in s)	Cryptographic time (in s)
1	ECG (Physionet.org 2016)	1150	5.2	3.6	8.8
2	EEG (Physionet.org 2016)	1690	2.4	2.3	6.7
3	UCD (Physionet.org 2016)	1050	1.6	1.4	3.0

Table 13 Comparison with the techniques stated at related works

Sl no.	Points on comparison	Atal and Singh (2020)	Lin et al. (2014)	Raeiatibanad-kooki et al. (2016)	Lin et al. (2016)	Murillo-Escobar et. al. (2017)	Proposed here
1	COVID-19 TMIS	Absent	Absent	Absent	Absent	Absent	Present
2	Multiple session keys formation	Absent	Absent	Absent	Absent	Absent	Present
3	Clinical ECG	Absent	Absent	Present	Absent	Present	Present
4	Clinical EEG	Absent	Absent	Absent	Absent	Present	Present
5	Clinical Echo	Absent	Absent	Absent	Absent	Present	Absent
6	Clinical UCD	Absent	Absent	Absent	Absent	Absent	Present
7	Signal storage used	Present	Present	Present	Present	Present	Present
8	Live streaming	Absent	Absent	Absent	Absent	Absent	Absent
9	Encryption technique	Present	Present	Present	Present	Present	Present
10	Application of metaheuristics	Absent	Absent	Absent	Absent	Absent	Present
11	Proposed fitness function	Absent	Absent	Absent	Absent	Absent	Present
12	Compression technique	Absent	Absent	Present	Absent	Absent	Absent
13	Intruding time detection	Absent	Absent	Absent	Absent	Absent	Present
14	Histogram	Absent	Absent	Absent	Absent	Present	Present
15	Autocorrelation	Present	Absent	Absent	Absent	Present	Present
16	Attack on plain signal	Absent	Present	Absent	Absent	Present	Present
17	Information entropy	Absent	Absent	Absent	Absent	Present	Present
18	Floating frequency	Absent	Absent	Absent	Absent	Present	Present
19	Quality metrics	Absent	Absent	Absent	Present	Present	Present
20	Noise attacks	Absent	Absent	Absent	Absent	Absent	Present
21	Occlusion attacks	Absent	Absent	Absent	Absent	Absent	Present
22	Cryptographic time	Absent	Present	Absent	Absent	Present	Present
23	Statement of comparison (Related Works)	Absent	Absent	Absent	Absent	Present	Present
24	Statement of result comparison (Earlier Works)	Absent	Absent	Absent	Absent	Absent	Present
25	Statement of comparison (Classical Algorithm)	Absent	Absent	Absent	Absent	Present	Present

9 Analysis on comparison

Cryptography based on chaotic functions was discussed in the above mention literature section (Murillo-Escobar et al. 2015; Awasthi and Srivastava 2013; Patidar et al. 2009; Murillo-Escobar et al. 2015; Khan et al. 2007). More papers were surveyed in that section. All the presented works have their limitations. Moreover, no paper in the literature survey section has dealt with different session keys in COVID-19 telemedicine. This paper has addressed this area with more security up gradation techniques. Telecare Medical Information System (TMIS) must indulge higher degree of data security features, so as to prevent the patients' data against different attackers. The following Table 13 contains a comparative statement when compared against the earlier works given in literature section. Thus, the efficiency of the proposed Post-COVID-19 TMIS can be observed in a tabular format.

The proposed technique has been compared with the classical cryptographic techniques viz. AES and triple DES (Patel 2019). The following Table 14 shows a comparative statement in this context.

10 Gap analysis

In this section, the gap analysis has been done. The objective of this section is to bridge the gaps which were present in the literature papers with our technique. The limitations of the related papers that were given in the literature section were noted in a tabular format. The following Table 15 has shown such limitations, and how the proposed technique had coped up with those limitations.

The following Table 16, a comparison on different result parameters between the proposed method and earlier methods has been displayed.

Table 14 Comparison with the classical cryptographic techniques

Sl. no.	Functional attributes	Triple DES	AES	Proposed here
1	Core Methodology	Fiestel Network	Substitution Permutation Network	Metaheuristic Salp Swarm
2	Key size	168	128 or 192 or 256	128
3	Key space volume	2^{168}	2128 or 2192 or 2256	2^{128}
4	Vulnerable attacks	Brute Force	Side Channel	Noise
5	Cryptographic time	Slower	Fast	Fast

Table 15 Limitations and proposed solution over earlier papers

Earlier authors' name	Limitation(s) of earlier papers	Our proposed remedies
Das et al. (2020)	No secured transmission of COVID-19 positive XRay detected cases	Security measures were carefully taken up through metaheuristic approach
Swapna et al. (2020)	They had not shown any cryptographic technique to transmit the cardiac signals	A novel encryption method to encrypt the cardiac data has been proposed
Apostolopoulos and Mpesiana (2020)	There should be secured way of transferring the decision from server to the users	Evaluation of the fitness of the salps leads to have higher degree of patients' data privacy
Murillo-Escobar et al. (2017)	The MITM attacks were not covered through their chaos based encryption	Different types of MITM attacks were resisted here. Histogram, floating frequency, autocorrelation, etc. would used in this regard
Lin et al. (2014)	Secret key generation concept was missing in their chaotic encryption of EEG signals	Metaheuristic session key has been designed with 128 bits length
Atal and Singh (2020)	Time needing to decode the cipher text by the intruders has not been mentioned	Brute-force attacks and others were mentioned in this manuscript
Capua et al. (2010)	The impact of telemedicine interface was not present	The proposed telemedicine architecture works on the salp swarm session key. It acts as robust key for myriad transactions
Ye et al. (2010)	Continuous heart rate monitoring needs tight security measures against different intruders	Different mathematical tests were conducted on the proposed technique to have more security on the cardiac data
Sarkar et al. (2020)	They had encrypted the ECG with limited mathematical tests	Noise attack, occlusion attack, plain text attack, plain signal attack, brute-force attack, etc. were conducted to have more efficacies

Table 16 Result comparison with other techniques

Test name	Earlier authors' name	Earlier result value	Our result value
Statistical fitness	Sarkar et al. (2020)	0.985437 (Monobit)	0.885 (Proposed)
Encryption time	Murillo-Escobar et al. (2014)	0.14 ms for 1126 character	5.2 s for 1150 (ECG), 2.4 s for 1690 (EEG), 1.6 s for 1050 (UCD)
Decryption time	Murillo-Escobar et al. (2014)	0.109 ms for 1126 character	3.6 s for 1150 (ECG), 2.3 s for 1690 (EEG), 1.4 s for 1050 (UCD)

Since, all the cryptographic papers have used different parametric tests on myriad secret keys and files to prove their efficacy. So on the results point of comparison, there could be only limited number of comparisons obtained in the above Table 16.

11 Conclusions, limitations and future scope

Keeping pace with the adaptability needed to cope up with the novel corona virus, the proposed method presented here is to critically identify a fittest session key from the salp population. The COVID-19 situations are getting worsen regularly. Thus, in the domain of Telecare Medical Information System (TMIS) (Bhowmik et al. 2019; Dey et al. 2021b, c), a patient can communicate their clinical signals without any hesitation to their physicians for diagnosis and regular follow-ups. The set of leader salps' coordinates generating the hash for 1035 iterations were passed through the said test with better efficacy. This proves the robustness of our proposed technique.

The proposed key generation technique using the salp swarm algorithm is a new dimension in fighting the COVID-19 plight. Metaheuristic based salp swarm algorithm is a problem independent technique to cater the needs of secured signal transmission in the global corona virus pandemic. Since this proposed technique deals with multiple session keys for the concurrent sessions, thus the intruders will not be able to damage all the sessions of the TMIS. Histogram, floating frequency and autocorrelation derived through the proposed technique propels the robustness of this proposed technique. Obtaining an expert opinion regarding the disease is a necessary condition before treatment. This can be efficiently done using the salp swarm based proposed technique of session key generation. Telecare Medical Information System embedded with such technique exhibits the security implications on the patients' confidential data. Cardiologists / doctors must be well equipped with the secured transmission

system and establish more scope of treatment skills. Resultant of such designed communication effective and reliable TMIS help to counter the security issues related in context of stealing of clinical signals in the middle (Dey et al. 2019; Sarkar et al. 2021). On the broader context of social welfare, the proposed technique serves as a key model with added dimensions particularly when the entire world is under the unprecedented challenge of corona virus.

The limitation of the proposed technique was that it dealt with cardiac related files of the patients. Patients' security is the foremost criterion in this TMIS. In the era of post-COVID-19 pandemic, patients are encouraged to stay at home and take telemedicine services from their isolates. Metaheuristic session key based encryption was done here in that regard. However, no genetic operations were taken into consideration. The involvement of genetic operations could enrich the security efficacy of the proposed COVID-19 Telecare Medical Information System.

Future scope of improvement of this proposed technique is to implement in a real time atmosphere. The patients' clinical signals would be sensed in live mode, and processed through chip based microcontroller before encrypting by the TMIS. In addition, the hardware security protocols are to be addressed intelligently while designing the circuit. From encryption point of view, to reduce the network traffic load and congestion, data compression techniques may be applied on the proposed technique too.

Acknowledgements Authors do acknowledge the moral and congenial atmosphere support provided by Maharajadhiraj Uday Chand Women's College, B.C. Road, Burdwan, West Bengal, India.

Funding Not applicable.

Declarations

Conflict of interest All the authors do declare that there is no conflict of interest.

Ethical approval This article does not contain any studies with human participants or animals performed by any of the authors.

References

- Abramowitz M, Stegun IA (1965) Handbook of mathematical functions with formulas, graphs, and mathematical tables. Dover
- Abualigah L, Shehab M, Alshinwan M et al (2020) Salp swarm algorithm: a comprehensive survey. *Neural Comput Appl* 32:11195–11215. <https://doi.org/10.1007/s00521-019-04629-4>
- Apostolopoulos ID, Mpesiana TA (2020) Covid-19: automatic detection from X-ray images utilizing transfer learning with convolutional neural networks. *Phys Eng Sci Med* 43:635–640. <https://doi.org/10.1007/s13246-020-00865-4>
- Atal DK, Singh M (2020) A dictionary matrix generation based compression and bitwise embedding mechanisms for ECG signal classification. *Multimed Tools Appl* 79:13139–13159. <https://doi.org/10.1007/s11042-020-08671-6>
- Awasthi AK, Srivastava K (2013) A biometric authentication scheme for telecare medicine information systems with nonce. *J Med Syst* 37(5):1–4.
- Bhowmik A, Dey J, Sarkar A, Karforma S (2019) Computational intelligence based lossless regeneration (CILR) of blocked gingivitis intraoral image transportation. *IAES Int J Artif Intell* 8(3):197–204
- Bokolo AJ (2021) Application of telemedicine and eHealth technology for clinical services in response to COVID-19 pandemic. *Health Technol* 11:359–366. <https://doi.org/10.1007/s12553-020-00516-4>
- Bokolo Anthony Jnr (2020) Use of telemedicine and virtual care for remote treatment in response to COVID-19 pandemic. *J Med Syst* 44:132. <https://doi.org/10.1007/s10916-020-01596-5>
- Borghetti M, Sardini E, Serpelloni M (2013) Sensorized glove for measuring hand finger flexion for rehabilitation purposes. *IEEE Trans Instrum Meas* 62:3308–3314
- Capua CD, Meduri A, Morello R (2010) A smart ECG measurement system based on web-service-oriented architecture for telemedicine applications. *IEEE Trans Instrum Meas* 59(2010):2530–2538
- Chaudhry SA, Mahmood K, Naqvi H, Khan MK (2015) An improved and secure biometric authentication scheme for telecare medicine information systems based on elliptic curve cryptography. *J Med Syst* 39(11):1–12
- Chen MJ, Bovik AC (2011) Fast structural similarity index algorithm. *J Real-Time Image Proc* 6:281–287
- Chen H-M, Lo J-W, Yeh C-K (2012) An efficient and secure dynamic ID-based authentication scheme for telecare medical information systems. *J Med Syst* 36(6):3907–3915
- Cowling PI, Kendall G, Soubeiga E (2002) Hyperheuristics: a tool for rapid prototyping in scheduling and optimisation. In: *Proceedings of the Applications of Evolutionary Computing on EvoWorkshops*, Springer, London, pp 1–10
- Cui D (2010) Chaotic secure content-based hidden transmission of biometric fourier transform. In: *International Conference on Machine Vision and Human-machine Interface*, 168–171
- Das AK, Goswami A (2013) A secure and efficient uniqueness-and-anonymity-preserving remote user authentication scheme for connected health care. *J Med Syst* 37(3):1–16
- Das AK, Goswami A (2014) An enhanced biometric authentication scheme for telecare medicine information systems with nonce using chaotic hash function. *J Med Syst* 38(6):1–19
- Das D, Santosh KC, Pal U (2020) Truncated inception net: COVID-19 outbreak screening using chest X-rays. *Phys Eng Sci Med* 43:915–925. <https://doi.org/10.1007/s13246-020-00888-x>
- de Oliveira Andrade A, Soares AB, de Andrade Palis A et al (2021) On the use of telemedicine in the context of COVID-19: legal aspects and a systematic review of technology. *Res Biomed Eng*. <https://doi.org/10.1007/s42600-021-00133-8>
- Dey J (2021) Pivotal “New Normal” Telemedicine: secured psychiatric homeopathy medicine transmission in Post-COVID. *Int J Inf Technol* 13:951–957. <https://doi.org/10.1007/s41870-021-00675-1>
- Dey J, Bhowmik A, Sarkar A, Karforma S (2019) Privileged authenticity in reconstruction of digital encrypted shares. *IAES Int J Artif Intell* 8(2):175–180
- Dey J, Bhowmik A, Sarkar A et al (2021a) Cryptographic engineering on COVID-19 telemedicine: an intelligent transmission through recurrent relation based session key. *Wireless Pers Commun*. <https://doi.org/10.1007/s11277-021-09045-3>
- Dey J, Sarkar A, Chowdhury B et al (2021b) Episode of COVID-19 telepsychiatry session key origination upon swarm-based metaheuristic and neural perceptron blend. *SN Comput Sci* 2:445. <https://doi.org/10.1007/s42979-021-00831-1>
- Dey J, Sarkar A, Karforma S (2021c) Newer post-COVID perspective: teledental encryption by de-multiplexed perceptrons. *Int J Inf Technol*. <https://doi.org/10.1007/s41870-020-00562-1>
- Elham Z et al (2011) Arrhythmia detection based on morphological and time-frequency features of T-wave in electrocardiogram. *J Med Signals Sens* 1(2):99–106
- Farr MA, Duvic M, Joshi TP (2021) Teledermatology during COVID-19: an updated review. *Am J Clin Dermatol* 22:467–475. <https://doi.org/10.1007/s40257-021-00601-y>
- Fatemian SZ, Hatzinakos D (2009) A new ECG feature extractor for biometric recognition. In: *16th International conference on digital signal processing*. IEEE, pp 1–6
- Garg P (2009) A comparison between memetic algorithm and genetic algorithm for the cryptanalysis of simplified data encryption standard algorithm. *Int J Network Security Appl* 1:34–42
- Gomes de Freitas FG, Brito MCL, Lima de Campos, GA, Teixeira de Souza J (2010) Optimization in software testing using metaheuristics. *Revista de Sistemas de Informação da FSMA*, 5, pp 3–13. 20
- Gopisetty R (2017) Automatic detection of cardiac arrhythmia through ecg signal analysis: a review. *IOSR J VLSI Signal Process* 7(6):1–12
- Hao X, Wang J, Yang Q, Yan X, Li P (2013) A chaotic map-based authentication scheme for telecare medicine information systems. *J Med Syst* 37(2):1–7
- Jiang Q, Ma J, Ma Z, Li G (2013) A privacy enhanced authentication scheme for telecare medical information systems. *J Med Syst* 37(1):1–8
- Jiang Q, Ma J, Lu X, Tian Y (2014) Robust chaotic map-based authentication and key agreement scheme with strong anonymity for telecare medicine information systems. *J Med Syst* 38(2):1–8
- Kahate A (2010) *Cryptography and network security*, 2nd edn. Tata McGraw Hill
- Karpagachelvi S, Arthanari M, Sivakumar M (2010) ECG feature extraction techniques-a survey approach. *Int J Comput Sci Inf Secur* 8(2010):76–80
- Karthigaikumar P, Anitha Christy N, Siva Mangai NM (2015) PSP CO₂: An efficient hardware architecture for AES algorithm for high throughput. *Wireless Pers Commun* 85(1):305–323
- Khajehzadeh M, Raihan Taha M, El-Shafie A, Eslami M (2011) A survey on meta-heuristic global optimization algorithms. *Res J Appl Sci Eng Technol* 3(6):569–578
- Khan M, Shah T (2014) A novel statistical analysis of chaotic S-box in image encryption. *3D Res* 5(3):1–8
- Khan MK, Zhang J, Tian L (2007) Chaotic secure content-based hidden transmission of biometric templates. *Chaos, Soliton Fract* 32:1749–1759
- Lee C-C, Hsu C-W (2013) A secure biometric-based remote user authentication with key agreement scheme using extended chaotic maps. *Nonlinear Dyn* 71:201–211
- Liaquat RM, Mehboob B, Saqib NA, Khan MA (2016) A framework for clustering cardiac patient’s records using unsupervised learning techniques. In: *The 6th International Conference on Current and Future Trends of Information and Communication Technologies in Healthcare (ICTH 2016)*. Elsevier

- Lin H-Y (2014) Chaotic map based mobile dynamic ID authenticated key agreement scheme. *Wireless Pers Commun* 78:1487–1494
- Lin C-F (2016) Chaotic visual cryptosystem using empirical mode decomposition algorithm for clinical EEG signals. *J Med Syst* 40(3):1–10
- Lin C-F, Shih S-H, Zhu J-D (2014) Chaos based encryption system for encrypting electroencephalogram signals. *J Med Syst* 38(5):1–10
- Liu N, Zhai G (2017) Free energy adjusted peak signal to noise ratio (FEA-PSNR) for image quality assessment. *Sens Imaging* 18:11. <https://doi.org/10.1007/s11220-017-0160-0>
- Lu Y, Li L, Peng H, Xie D, Yang Y (2015) Robust and efficient biometrics based password authentication scheme for telecare medicine information systems using extended chaotic maps. *J Med Syst* 39(6):1–10
- Mahmoodabadi S, Ahmadian A, Abolhasani M, Eslami M, Bidgoli J (2006) ECG feature extraction based on multiresolution wavelet transform. In: 27th Annual International Conference of the Engineering in Medicine and Biology Society, IEEE, pp 3902–3905
- Manda K, Satapathy SC, Poornasatyanarayana B (2012) Population based meta-heuristic techniques for solving optimization problems: a selective survey. *Int J Emerg Technol Adv Eng* 2(11):206–211
- Mirjali S et al (2017) Salp Swarm Algorithm: a bio-inspired optimizer for engineering design problems. *Adv Eng Softw* (elsevier) 114:163–191
- Mulyadi IH, Nelmiawati ES (2019) Improving accuracy of derived 12-lead electrocardiography by waveform segmentation. *Indones J Electr Eng Info* 7(1):15–21
- Murillo-Escobar MA, Abundiz-Perez F, Cruz-Hernandez C, Lopez-Gutierrez RM (2014) A novel symmetric text encryption algorithm based on logistic map. In: Proceedings of the International Conference on Communications, Signal Processing and Computers, pp 49–53
- Murillo-Escobar MA, Cruz-Hernandez C, Abundiz-Perez F, Lopez-Gutierrez RM (2015a) A robust embedded biometric authentication system based on fingerprint and chaotic encryption. *Expert Syst Appl* 42:8198–8211
- Murillo-Escobar MA, Cruz-Hernandez C, Abundiz-Perez F, Lopez-Gutierrez RM, Del Campo ORA (2015b) A RGB image encryption algorithm based on total plain image characteristics and chaos. *Signal Process* 109:119–131
- Murillo-Escobar MA et al (2017) A double chaotic layer encryption algorithm for clinical signals in telemedicine. *J Med Syst* 41:59
- Nan J, Jia R, Meng S et al (2021) The impact of the COVID-19 pandemic and the importance of telemedicine in managing acute ST segment elevation myocardial infarction patients: preliminary experience and literature review. *J Med Syst* 45:9. <https://doi.org/10.1007/s10916-020-01703-6>
- Parejo JA, Ruiz-Cortés A, Lozano S et al (2012) Metaheuristic optimization frameworks: a survey and benchmarking. *Soft Comput* 16:527–561. <https://doi.org/10.1007/s00500-011-0754-8>
- Patel K (2019) Performance analysis of AES, DES and Blowfish cryptographic algorithms on small and large data files. *Int J Inf Technol* 11:813–819
- Patidar V, Pareek NK, Sud KK (2009) A new substitution-diffusion based image cipher using chaotic standard and logistic maps. *Commun Nonlinear Sci* 14:3056–3075
- Peden CJ, Mohan S, Pagán V (2020) Telemedicine and COVID-19: an observational study of rapid scale up in a US Academic Medical system. *J Gen Intern Med* 35:2823–2825. <https://doi.org/10.1007/s11606-020-05917-9>
- Physionet.org (2016) PhysioBank ATM. Online, Available on <https://physionet.org/cgi-bin/atm/ATM>. Accessed Nov 2020
- Raeiatibanadkooki M, Quchani SR, KhalilZade M, Bahaadinbeigy K (2016) Compression and encryption of ECG signal using wavelet and chaotically huffman code in telemedicine application. *J Med Syst* 40(3):1–8
- Sageena G, Sharma M, Kapur A (2021) Evolution of smart healthcare: telemedicine during COVID-19 pandemic. *J Inst Eng India Ser B*. <https://doi.org/10.1007/s40031-021-00568-8>
- Samanta S, Chakraborty S (2011) Parametric optimization of some non-traditional machining processes using artificial bee colony algorithm. *Eng Appl Artif Intell* 24(6):946–957
- Sarkar A, Dey J, Bhowmik A, Mandal JK, Karforma S (2019a) Computational intelligence based neural session key generation on E-health system for ischemic heart disease information sharing. In: Mandal J, Sinha D, Bandopadhyay J (eds) Contemporary advances in innovative and applicable information technology. Advances in intelligent systems and computing, vol 812. Springer, Singapore
- Sarkar A, Dey J, Chatterjee M, Bhowmik A, Karforma S (2019b) Neural soft computing based secured transmission of intraoral gingivitis image in E-health. *Indones J Electr Eng Comput Sci* 14(1):178–184
- Sarkar A, Dey J, Karforma S (2020) Secured session key-based E-Health: biometric blended with salp swarm protocol in telecare portals. In: Mandal J, Mukhopadhyay S (eds) Proceedings of the global AI Congress 2019. Advances in intelligent systems and computing, vol 1112. Springer, Singapore
- Sarkar A, Dey J, Karforma S (2021) Musically modified substitution-box for clinical signals ciphering in wireless telecare medical communicating systems. *Wireless Pers Commun*. <https://doi.org/10.1007/s11277-020-07894-y>
- Segura C, Hernandez A, Luna F, Alba E (2017) Improving diversity in evolutionary algorithms: new best solutions for frequency assignment. *IEEE Trans Evol Comput* 21:539–553. <https://doi.org/10.1109/TEVC.2016.2641477>
- Setiadi DIM (2021) PSNR vs SSIM: imperceptibility quality assessment for image steganography. *Multimed Tools Appl* 80:8423–8444. <https://doi.org/10.1007/s11042-020-10035-z>
- Stangierski J, Weiss D, Kaczmarek (2019) A multiple regression models and artificial neural network (ANN) as prediction tools of changes in overall quality during the storage of spreadable processed Gouda cheese. *Eur Food Res Technol* 245:2539–2547. <https://doi.org/10.1007/s00217-019-03369-y>
- Swapna MS, Renjini A, Raj V et al (2020) Time series and fractal analyses of wheezing: a novel approach. *Phys Eng Sci Med*. <https://doi.org/10.1007/s13246-020-00937-5>
- Talbi EG (2002) A taxonomy of hybrid metaheuristics. *J Heuristics* 8(5):541–564
- Wang Z, Huo Z, Shi W (2015) A dynamic identity based authentication scheme using chaotic maps for telecare medicine information systems. *J Med Syst* 39(1):1–8
- WHO (1998) A health telematics policy in support of WHO's Health-For-All strategy for global health development report of the WHO group consultation on health telematics. World Health Organization, 11–16 December, Geneva, Switzerland
- Willmott C, Matsuura K (2005) Advantages of the Mean Absolute Error (MAE) over the Root Mean Square Error (RMSE) in assessing average model performance. *Clim Res* 30:79–82
- Yan X, Li W, Li P, Wang J, Hao X, Gong P (2013) A secure biometrics-based authentication scheme for telecare medicine information systems. *J Med Syst* 37(5):1–6
- Yang X-S (2014) Nature-inspired optimization algorithms. Elsevier BV, pp 23–44. <https://doi.org/10.1016/b978-0-12-416743-8.00002-6>
- Ye C, Coimbra MT, Kumar BV (2010) Investigation of human identification using two-lead electrocardiogram (ECG) signals. In: 2010 Fourth IEEE international conference on biometrics: theory applications and systems (BTAS), IEEE, pp 1–8

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.