J. Inst. Eng. India Ser. B (August 2022) 103(4):1127–1146
https://doi.org/10.1007/s40031-022-00711-z

ORIGINAL CONTRIBUTION

Episode of Dual Neural Genetic Firefly (DNGF) Transmission Key Generation in New Normal Mode of COVID-19 Second Wave Telepsychiatry

Joydeep Dey[1] · Sunil Karforma[2] · Bappaditya Chowdhury[3]

Received: 2 June 2021 / Accepted: 3 January 2022 / Published online: 31 January 2022

Abstract The volume of E-commerce transactions had accelerated on huge scale due to COVID-19. Telemedicine comes under the segment of E-commerce, where the patients can get their treatments from isolates. Patients' information security is a basic challenge in this COVID-19 telemedicine segment. The majority of the non-obtrusive and non-emergency patients are encouraged and treated distantly from their secludes without the inclusion of COVID-19 transmission. Anxiety, depressive disorders, stress, dementia, mood disorder, OCD, aggression, etc. are the critical mental challenges that have abruptly occurred during this COVID period. The present work focused on "New Normal Mode" of COVID-19 telepsychiatry so that the patients' mental illness can be treated remotely in a secure way. An episode of dual neural-genetic firefly (DNGF) has been proposed on COVID-19 "New Normal Mode" 2nd wave telepsychiatry. The pool of transmission keys was generated with the help of firefly algorithm, neural perceptron, and genetic operations. Besides these, the proposed DNGF keys are effective to be used for different online psychiatric transactions. The objectivity of this paper is to generate a robust pool of transmission keys in order to nullify different types of intruding. It has effectively cleared Avalanche test and Strict Avalanche test. The outcome of parameterized functional security test has been recorded with adequacy. These were: 0.327933, 0.350467, 0.332533, 0.317867, and 0.350267 on the generated pool of DNGF. The correlation coefficient between the key generation time and parameterized functional security has been found to be $r_{GT,FS} = -0.53404$. Distinctive mathematical arranged examinations were directed on the proposed key pool. It has shown better reasonability on the part of the COVID-19 2nd wave telepsychiatry, which is a component of E-commerce.

Keywords Telepsychiatry · Dual neural genetic firefly (DNGF) · Key generation time · Statistical test

Abbreviations

AES	Advanced Encryption Standard
COVID-19	Corona Virus Disease 19
DES	Data Encryption Standard
DNGF	Dual Neural Genetic Firefly
E2E	End-to-End
E-Commerce	Electronic Commerce
FA	Firefly Algorithm
FSP	Functional Security Parameter
GA	Genetic Algorithm
HIPAA	Health Insurance Portability and Accountability Act
IDEA	International Data Encryption Algorithm
MMD	Major Mental Disorder
OCD	Obsessive–Compulsive Disorder
OPD	Out Patient Department
RC5	Rivest Cipher 5
RC6	Rivest Cipher 6

✉ Joydeep Dey
joydeepmcabu@gmail.com

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

[2] Department of Computer Science, University of Burdwan, Burdwan, India

[3] Department of Psychiatry, AMRI Hospital, Salt Lake, Kolkata, India

Introduction

The tale COVID-19 has incited to have changes in all circles of day-by-day life. Acclimatization has been affected in the domain of E-commerce as well. As of now, it has been seen the second wave of this deadly coronavirus with more destructive variations. People have been restricted inside their homes. Online shopping has been very much active in this scenario. Telemedicine has also been a part of e-commerce services. It prevents the transmission rate of this virus. Patients have been limited to Out Patient Department (OPD) visits. Emergency clinics and clinical chambers have effectively abridged such administrations and facilities. Selecting clinical benefits from remote telemedicine has arisen as the most ideal choice to oppose the COVID-19 transmission. In this worldwide COVID-19 pandemic, telemedicine has contributed a great deal towards treating the patients by withstanding the standards of social distance and lockdown. Arrangement of online follow-ups had prompted and served the non-emergency and non-obtrusive patients distantly [1]. Since due to different pandemic critics, mental illness has raised a lot. Extended variations in mental conditions were observed in this pandemic. Such critical challenging issues were Insomnia, Anxiety, Severe Depression, Aggression, OCD, MMD, delusion, phobia, etc. Thus, to treat psychiatric patients, telepsychiatry could be another effected tool. This is the principle motivation behind telepsychiatry in COVID-19 2nd wave "New Normal Mode" period.

PCs, Internet networks, smartphones, switches, routers, workstations, and so on are the equipment segments of telepsychiatry. Through these segments, the patients' present body status can be monitored by the specialists [2]. Fraudsters do consistently stay dynamic to get a handle on the patients' clinical information during the online transmission. Public channels are more hazardous to the patients and specialists. To oppose against such assaults is a serious deal while fostering the security conventions of such COVID-19 telepsychiatry. After the execution of lockdown, the information volumes on telepsychiatry have unexpectedly flown over. The capacity of telepsychiatry had supported the virtual visits to the psychiatrists for the non-crisis patients. Moreover, telemedicine comes under the category of emergency E-commerce services in the lockdown period. Also, co-morbid patients were more inclined to the COVID-19. So they could likewise be dealt with distantly as they need normal observing and subsequent follow-ups. Likewise, telemedicine administrations can deal with to minimization of COVID-19 transmission [1, 3].

To guarantee psychiatric patients' data security, cryptography is the most fit device that can be applied on COVID-19 telepsychiatry. There exists two broad types of cryptography. They are Symmetric key cryptography and Asymmetric Key Cryptography. Symmetric key cryptography is the designing method to change the plain content into ciphertext with a mysterious secret key. The marvel of information encryption is done at the sender's end and decoding at the beneficiary's end. Same secret key is used in such symmetricity. Appropriate consideration ought to be received for the choice of the transmission key. Its point is to give greater classification on the patients' clinical information in this electronic COVID-19 telepsychiatry [4–6]. Just the approved clients can log-inside, send information, get information and approve the reports. Fraudsters are a lot of dynamic on COVID-19 patients' information for manipulation purpose. During this pandemic, the clinical exchanges colossally spilled inside the online organizations. Fraudsters snatch such private information for various unlawful things. The existing architecture of COVID-19 telepsychiatry has been presented in the following Fig. 1.

Figure 1 describes the existing architecture of COVID-19 telepsychiatry. The chief problem in the above architecture lies in the data security of psychiatric patients. As intruders can easily sniff the private medical data from the open networks, so such data must be preserved carefully during the open transmission. Due to this security issue, patients are not comfortable to opt for telepsychiatry. This paper has mainly addressed this critical data challenge amidst COVID-19 2nd wave using neural networks and metaheuristic approaches.

Metaheuristic calculations were presented by mimicking the common species to speed up the arrangement looking through wonder. Its goal is to investigate the pursuit space and to reach closest optimum solution. Such arrangements are by and large rough qualities with non-deterministic properties. Firefly calculation was additionally evolved by

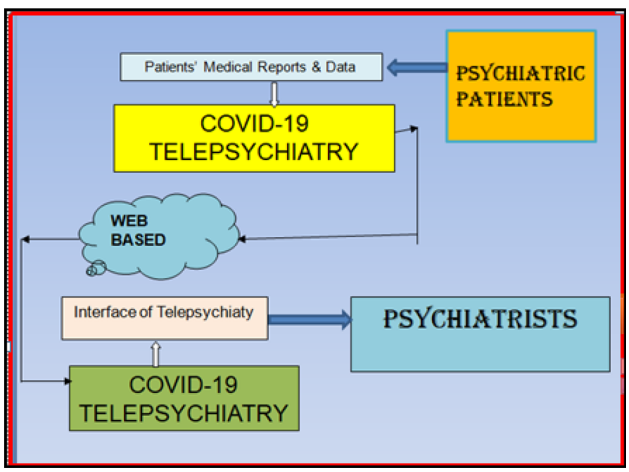

Fig. 1 COVID-19 telepsychiatry: existing architecture

the recreation of the firefly developments. This paper presents Dual Neural Genetic Firefly (DNGF) transmission key arrangement by manipulating the conduct of the firefly [7]. The accompanying Table 1 addresses the connection between the metaheuristics and cryptographic engineering upon various properties.

In Table 1, it has been pointed out the connection points between the metaheuristic algorithms and cryptographic engineering techniques. The background concept of metaheuristic algorithms is nature-inspired species, while mathematical and statistical concepts are for cryptographic engineering. The internal requirements of both types of methods are food foraging and secret key generation respectively. Local and global search criterion is present in metaheuristic algorithms whereas, pseudorandom sequencing is more common in cryptographic tools. A balance has been made between the control of exploration and exploitation variables with the help of myriad secret key lengths. The complexity depends on the complexity of the structures and algorithms of the metaheuristic and cryptographic algorithms respectively.

The prime motivation behind the development of this proposed technique is as follows. Psychiatric patients would be tremendously be profited from COVID-19 telepsychiatry framework. Although in the last few years, lots of methods were designed. But most of them suffered the problem of patients' data security and privacy. Telepsychiatry faced a critical challenge in the form of data secrecy. The proposed technique has filled that gap to a large extent. It empowers the patients to abridge the voyaging expenses to the hospitals and body's mileage. They may effectively send clinical reports and medical data to the psychiatrist through remote COVID-19 telepsychiatry [8]. It has been considered as the safest way to get treated for the COVID patients and allied patients from their home quarantines. The chances of COVID-19 attack through COVID-19 telepsychiatry are absolutely zero. Besides, the psychiatrists may likewise transmit something to her / his researchers, seniors, and so forth for research reasons or others. Gatecrashers sitting inside the middle organizations may take the patients' secret information, and they tenaciously contort or alter them for negative purposes. Dual Neural Genetic Firefly (DNGF) transmission key is the most striking commitment in this proposed methodology.

Background

Urge of COVID-19 Telepsychiatry

In the second wave, the mortality rate is higher than first wave of coronavirus [8, 9]. Keeping the safety measurements, mental care treatment has stepped fast towards digital methods i.e. telepsychiatry, so that the patients, psychiatrists, hospital staffs are not subject to COVID-19 risk. Telepsychiatry consultations can play a pivotal role because it gets the opinion and treatments from the psychiatrists. Mental illness can be addressed in that way by abiding by the COVID-19 protocols [10]. In telepsychiatry, the protocols of lockdown can be followed well [11, 12]. Mahmoud et al. [13] have defined the usage of Internet-based technologies likes video call, phone calls, chats, etc. in order to provide better mental care to the patients in this pandemic. It is a matter of true fact that telepsychiatry has emerged as a compulsory organ to treat psychological patients remotely. Telemental health care support can

Table 1 Association between the Metaheuristics and Cryptographic Engineering

Serial Number	Properties	MetaheuristicAlgorithms	Cryptographic Engineering	Association Descriptions
1	Background	Natured Inspired Species	Mathematics & Statistics	Nature-inspired optimization techniques have been developed mathematically and statistically both
2	Internal Requirement	Food foraging by species	Secret key generation	Species food hunt has been simulated to find the fittest species as fittest session key
3	Search Solution	Local and global search	Pseudorandom sequence	A highly randomized sequence has been generated within the global search space domain
4	Control Strategy	Control of exploitation and exploration variables	Secret Key length	To maintain a balance between the variables and developing ciphertexts using different variety of secret keys
5	Complexity	On structures	On algorithm	Since metaheuristics search approaches are non-straight in style. Along these lines, fittest cryptographic key can be created utilizing this methodology which thus gives randomness and strength and upgrades the security protocol

extend its facilities to all the persons having any psychological complications. In the context of present COVID-19, it has been extremely helpful to such patients. They can get their virtual consultations from their quarantines [14]. Hau et al. [15] had assessed the positives of telepsychiatry on geriatric patients during coronavirus time. They are at the most risky states amid COVID-19. Such telepsychiatry services always can reduce the different psychiatric complications. They can remotely avail these services. Moreover, geriatric patients with co-morbidity are at the highest zone of mortality. They are advised more not to go outside their homes unless extreme emergency. Patients' teleconsultations with their psychiatrists can be made secured in procured way [16].

Cryptography in E-Commerce

In the current times of COVID pandemic, the utilization of E-commerce has been extended exponentially. Cryptographic arrangement is a piece of planning that manages message affirmation, so it gets undefined by outer entities and can be taken part in open channel public correspondence. It is the science to impose security mechanisms on various modes of data. Various types of encryption and mathematical calculations are made to overwhelm the enemies. In simple words, the opponents are made hard to read those ciphered texts. Chiefly, the plain content is changed over into figure text utilizing an encryption calculation, with the goal that the gatecrashers can't understand it. Regardless, confirmed gatherer beneficiary can essentially get to it by disentangling it on the other hand. The unscrambling calculation works on the contrary sales and converts the code text into plain content at the beneficiary end in the opposite activity. Such security parameters are compulsory in any kind of online trading. Two general sorts of cryptography are available. They are symmetric key cryptography and asymmetric key cryptography [17–20]. This paper has been executed on the symmetric key cryptography over COVID-19 telepsychiatry. Symmetric key cryptography has bigger throughput against awry key cryptography. Some of existing symmetric key cryptography techniques are IDEA, AES, DES, 3 DES, RC5, RC6 [21, 22]. The security mechanism between the vendors and the clients in E-commerce were fully supported by the cryptographic calculations. If no security is imposed, then the clients' sensitive data will be exposed to external opponents.

Session Key Concept

Session key is a groundbreaking code that is utilized at the encryption and deciphering measure in any data correspondence [23, 24]. In symmetric-key cryptography, the same session key is utilized by the source and destination. In this manner, such frameworks are savvier to conflict with the fraudsters. In COVID-19 telepsychiatry, the transmission key is especially needful to have online exchange by the patients and the psychiatrist. It ought to be dynamic concerning time. In this pandemic, multiple session key-streams were proposed to ensure secured CT scan encryption. CT scan has been used to find out the COVID infections inside the patients [25]. The session key must be arranged and handled with precision. It signifies the confidentiality of the patients' sensitive data. Moreover, authentication and key agreement is also needed [26]. In that respect, Mitev et al. [27] had proposed a secret key generation method on wireless systems. Researchers are engaged in developing new set of secret keys with enriched functionalities [28, 29]. It may also include biometric session keys [30].

Related Works

This segment reviews the existing works with respect to the proposed techniques of DNGF transmission key generation. The whole segment has been categorized under the following sub-sections. In the first sub-Sect. 3.1, related papers on COVID-19 telepsychiatry were reviewed. The related works on metaheuristic firefly algorithm were reviewed in the last sub-section.

Works on COVID-19 Telepsychiatry

This section deals with the literature survey. It has been briefly mentioned with respect to our proposed technique. Monaghesh et al. have surveyed different COVID-19 research papers on telehealthcare. They had observed that telehealth is having much potential to deal with different challenges faced in the light of COVID-19 pandemic. It has reduced the direct contact with patients and the doctors inside the community [31]. Brien et al. have discussed the technological usage in the treatment of COVID-19 psychiatric patients through digital platforms. Technical advancements have been a boom in this critical situation to deal with remote patients. Telepsychiatry treatment has been possible in this unprecedented crisis by avoiding physical visits [32]. Antony et al. have studied many papers related to COVID-19 telemedicine. Telemedicine and virtual care platforms are other emerging source for medical service providers. Through this online virtual care, patient monitoring, follow-ups, diagnosis, treatments, counseling, etc. can be done easily in the era of COVID-19 [33]. Gautam et al. [34] have reviewed papers and found that COVID-19 warriors are more prone to psychiatric issues, especially in females. They have cited the more relevance

of telemedicine in treating such mental issues in this pandemic situation. Their study was on the impact of coronavirus on mental health in USA. Stoll et al. [35] have discussed different ethical issues related to telepsychiatry in COVID-19. Psychiatrists may be guided with the protocols of standards of mental care support in treating the vulnerable COVID 19 patients. Smith et al. [36] had generated a comprehensive guidelines summary related to the telepsychiatry to cope up with COVID-19. It helps the psychiatrists to take safety measures while doing online treatments. Digital technology is an important component in telepsychiatry. Rezaeibagha et al. [37] have proposed a symmetric key-based telemedicine system protocol. Here the patients can avail the health care facilities from different locations. They had emphasized the security parameters likes of patient data confidentiality, anonymity and data integrity of the patients, and mutual authenticity. Dey [8] had proposed a pivotal way of transmitting homeopathic psychiatric medicines to patients. The author's work had been mainly emphasized the security aspects of the patients during the post-COVID-19 era.

Works on Metaheuristic Firefly algorithm

Yang et al. [38] had utilized the firefly calculation to take care of the improvement issues. Additionally, they had proposed new test work having stochastic or peculiarity parts which are more appropriate for issue approval. Chao et al. [39] had planned a spiral premise work network dependent on firefly calculation to arrange various sorts of supraspinatus sicknesses. Ultrasound pictures are being characterized into four classes of typical, ligament tears, ligament irritation, and calcific tendonitis. Apostolopoulos et al. [40] had planned firefly calculation to settle multi-objective load dispatch monetary discharge issue. They had created similar yields as for existing nature enlivened calculations. Jati et al. [41] had applied the firefly calculation to get the arrangement of mobile sales rep issue. Karthikeyan et al. [42] had proposed a crossbreed discrete firefly calculation for tackling the adaptable occupation booking issue. Here, the discrete firefly calculation and neighborhood search were joined together to acquire upgraded results. Senthilnath et al. [43] had utilized the firefly calculation to tackle two benchmark issues, at that point contrasted and Particle Swarm Optimization and Artificial Bee Colony. Veeramuthu et al. [44] had proposed to arrange the clinical pictures of Computed Tomography (CT) with remarkable highlights dependent on the firefly procedure.

Rani et al. [45] had designed an indispensable image compression technique. They had involved Particle Swarm Optimization (PSP) and Firefly Algorithm (FA) to have decent quality images. They had shown an improvement of 1.2–6 dB with respect to other compression methods. Talib et al. [46] had investigated an intelligent optimizer named as advanced firefly algorithm to calculate the proportional-integral-derivative (PID) controller in case of semi-active suspension things. Notable improvisation was observed in their technique because it had the reducibility of amplitude of the sprung acceleration to 56.5% and body acceleration to 67.1%. Fan et al. [47] had developed a new mutant of Firefly Algorithm (FA) for double stage mixed flow shop scheduling algorithm. Their simulation results had shown higher convergence rates and better efficacy of calculating the workloads. Alomoush et al. [48] had proposed a new automated segmentation method based on fuzzy c-means combined with Firefly Algorithm. Other conventional fuzzy c-means methods suffered from different drawbacks. They have minimized the risk of trapping into the local optimum solution. Their results were brilliant when compared against the existing algorithms. Anuradha et al. [49] had presented a novel combination of Differential Evolution and Firefly Algorithms for conducting the clustering works in an organized manner. Their effectiveness had been achieved through results when compared with other earlier techniques. Vinothini et al. [50] had proposed an Iterative Proximal Algorithm for the load balancing purpose. They had used firefly algorithm on multiple servers to balance their loads. They had improved the load balancing performance the computational skills of the task submitted by different users. Many results were taken by their study. Meena et al. [51] had designed two algorithms based on modified firefly in the context of updation equation with higher accuracy values.

Contemporary Priority Emphasis

The present work manages the issues associated with most elevated need in the time of COVID-19 computerized telepsychiatry. In the COVID-19 telepsychiatry, the issue of patients' associated reports and information at the hour of public media transmission is the greatest contemporary challenge seen here. In this saturated COVID-19 telehealth, the clinical information relating to online transactions is the most vulnerable [52–54]. These medical transactions are mostly inclined to the Man-In-The-Middle attacks. Intruders will control and alter the patients' information for their illicit benefits and medi-claims. The patients and the

physicians have bigger likelihood of getting caught into legitimate questions by virtue of these fraud assaults. Legal, as well as financial litigations, may be incurred on the patients' and doctors' end. Also, monetary misfortunes will bring about during the online expenses receipts or installments. In such cases, intruders will move the exchange add up to their record by pretends. An absence of patients' login validation from the whole COVID-19 telepsychiatry papers has been noted carefully. The transmission key can be compromized due to various organization faults. Such causes might be spillage of public correspondence medium, compromized channel, catching patients' or doctors' hubs, etc. Consequently, intruders can pretend effectively and speak with the customers for their benefit. It is another important issue that should be emphasized. Because of executions of re-lockdown in the subsequent second wave, the patients are encouraged to select online clinical help. Such exchanges have risen dramatically since the time of the appearance of novel COVID-19. Equal fraudsters' assaults have additionally quickly expanded in numbers. No paper has been found to have metaheuristic approach to have key generation in COVID-19 wave two telepsychiatry period.

Telepsychiatry Security Concerns

The authors have tried to point out certain security concerns over the COVID-19 telepsychiatry. As we know that patients' medical data are the most sensitive in nature. They must be protected from opponent usage and manipulations. Following are the key points that could be maintained in any COVID-19 telepsychiatry.

- Psychiatrists must ensure to have a secured and trusted web platform for video calls.
- They should also ensure that the audio and video transmission must strongly be encrypted with session keys.
- In case of text chat, psychiatrist must use End-to-End (E2E) chat platforms.
- Authentication should be present in the COVID-19 telepsychiatry system. Thus, actual users can only use the system.
- The local devices should not store any patients' medical data. However, it stored for research purpose, it should be encrypted in a different format.
- Systems must be enabled with antivirus software, and frequent updates are mandatory for its proper functionality.
- Consistence with Health Insurance Portability and Accountability Act (HIPAA) is fundamentally required [55, 56]. HIPAA sets a base government standard for the security of telemedicine data. Different countries may likewise set security laws that can be considerably more severe, so make certain to check any important rule for that country state wherein located. Just on the grounds that product says that HIPAA-consistent isn't sufficient to deliver.
- Multiple session keys should be implemented for different transactions.

Proposed Block Diagram

The proposed block diagram of DNGF transmission key in COVID-19 2nd wave telepsychiatry is shown in Fig. 2.

In the Fig. 2, double neural perceptrons were used. These would, in turn, generate two different weight vectors. Furthermore, genetic operation has been offered on these two neural weight vectors. Then weight vector of the firefly algorithm gets initialized to run that proposed algorithm. The outcome of this procedure is the generation of the Dual Neural Genetic Firefly (DNGF) transmission key. This key has been used in the COVID-19 second wave of telepsychiatry.

Traditional Firefly Algorithm

Firefly Algorithm (FA) is a nature-inspired algorithm which is based on the flashing attribute of firefly.

Genuine arbitrary numbers are utilized in this methodology for open correspondence between the fireflies. Henceforth, it very well may be utilized to settle multi-objective problems [38, 57, 58]. Following three points are the superb parts of this traditional firefly algorithm. They are as per the following.

a) More blazing fireflies will draw in less glimmering fireflies, regardless of their sex,
b) Degree of fascination is straightforwardly identified with its brilliance, and contrarily identified with the distance among them, and

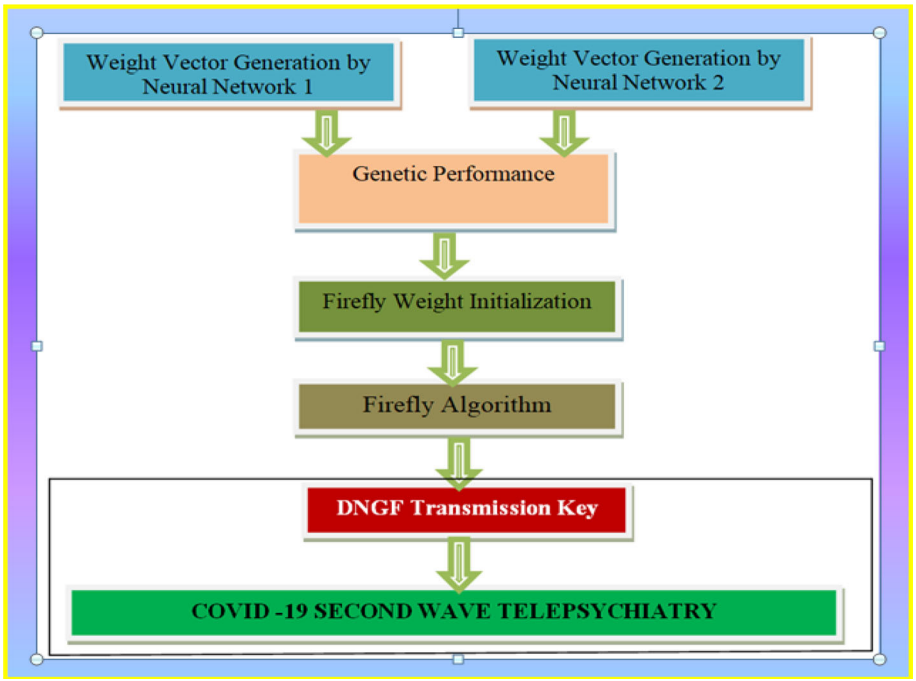

Fig. 2 Block diagram of the proposed technique

c) Brightness of the firefly is the outcome of fitness function and is dynamic concerning problem-based issues [57].

The attractiveness of each participating firefly can be calculated by using the following monotonic decreasing function 1. The attractiveness decreases with the rise in the distance between the fireflies.

$$\text{Attraction}(\text{Ed}) = \text{Attraction}_0^{'} * (-\text{Al} * \text{Ed}^p) : p \geq 1 \quad (1)$$

Here, Ed denotes the distance between two fireflies, $\text{Attraction}_0^{'}$ is the initial value of attraction at Ed = 0, Al is the standard absorption coefficient of light. The distance may be calculated in terms of Euclidean distance which has been mentioned in the following equation number 2.

$$Ed_{i,j,k} = \sqrt{(x_i - x_j - x_k)^2} + (y_i - y_j - y_k)^2 + (z_i - z_j - z_k)^2 \quad (2)$$

For the mating reason, less flashing fireflies will move towards the more flashing fireflies. It can be stated in the following Eq. 3.

$$L_i = L_i + \text{Attraction}_0^{'} * \left(-Al * Ed_{i,j,k}^2\right) * (L_j - L_i) + \propto 1 * \text{RNG}(-1/2) \quad (3)$$

Here, L is the present location, $Attraction_0^{'} * \left(-Al * Ed_{i,j,k}^2\right) * (L_j - L_i)$ denotes attractive determination criteria, and $\propto 1 * RNG(-1/2)$ denotes the randomized firefly movement when no more brighter fireflies are present. $\propto 1$ and RNG() are the initial constant value and random generator as per problem demands.

Significant Novelties of the proposed DNGF

In the phase of second wave of coronavirus, protection must be taken more to counter-attack the COVID attacks. In various parts, re-imposed lockdown has been done. This paper deals with the security parameters of the patients. Psychiatric patients' medical data need to be communicated through public channel in a secured way. Here it has been formulated a secure way to generate dual neural-genetic firefly (DNGF) transmission key. Following are the significant novelties of the proposed COVID-19 telepsychiatry. It includes the patients' data privacy aspects in the context of E-commerce.

- Security aspect in E-commerce segment as COVID-19 telepsychiatry.

- Due to COVID-19, online commercial transactions have immensely raised. So the proposed technique generates dynamic session key for encryption.
- Firefly Algorithm based on neural networks and genetic operation to ensure higher security.
- Many dual neural-genetic firefly (DNGF) transmission keys were generated for COVID-19 telepsychiatry.
- Genetic operations involved in the neural weight vectors. Thus, intruder will not be able to detect the pattern of the weight vector.
- Metaheuristic firefly COVID-19 telepsychiatry has been emphasized to generate the DNGF key pool set.
- Parameterized functional security outcome has been derived on each DNGF.
- Security enrichments in the domain of E-commerce have been analyzed.

X-axis, Y-axis, and Z-axis coordinates. For considering a randomized weight vector, we have used dual artificial neural networks. Two perceptrons were simulated to generate their respective weight vectors. Then genetic operation was incorporated to make more robust. The end product of the genetic operation has been concatenated to feed into the firefly algorithm. The stipulated fitness of each of the participating firefly may be used dynamically as per the problem demands. The weight vectors were sorted after each epoch, and the brighter firefly would move towards the less bright participating firefly. Multiple transmission keys for the unique telepsychiatry COVID-19 have been generated. The following algorithm will describe the proposed (DNGF) transmission key generation.

Proposed Algorithm 1: Dual Neural Genetic Firefly (DNGF) Transmission Key Generation in COVID Telepsychiatry

$\boldsymbol{Input(s)}$: $Number\ of\ Fireflies: N, Maximum\ Iteration, In\ \ E-Prescription: E.pdf$
$\boldsymbol{Output(s)}$: $Pool\ of\ DNGF\ Transmission\ Keys$
$/*\ Generation\ of\ Proposed\ Weight\ Vector\ */$
$X_i = \boldsymbol{Call\ Dual\ Nero-Genetic\ Vector}\ ()$
$/*\ Assigning\ Firefly\ Coordinates\ */$
$While\ (i < N)$
$N[i][0] \leftarrow Xcoordinate()$
$N[i][1] \leftarrow Ycoordinate()$
$N[i][2] \leftarrow Zcoordinate()$
$Set\ i = i + 1$
$End\ while$
$/*\ Fitness\ function\ Check\ */$
$For\ i = 0\ to\ N$
$F[i] \leftarrow \boldsymbol{CallFitness}\ (\boldsymbol{N[i]})$
$End\ for$
$Epoch \leftarrow 0$
$While\ (Epoch\ != In)$
  $For\ i = 0\ to\ N$
    $For\ j = 0\ to\ N$
      $If\ (\boldsymbol{Call\ Fitness(N[j])} < \boldsymbol{Call\ Fitness(N[i])})\ Then$
        $Move\_Firefly(N[j], N[i])$
      $End\ if$
    $End\ for$
  $End\ for$
$For\ i = 0\ to\ N$
  $F[i] \leftarrow \boldsymbol{CallFitness}(\boldsymbol{N[i]})$
$End\ for$
$Epoch = Epoch + 1$
$End\ while$

Proposed Technique

This technique deals with the formation of Dual Neural Genetic Firefly (DNGF) transmission keys for COVID-19 2nd wave telepsychiatry. It has been assisted by the genetic support on the neural-based metaheuristic firefly method. Initially, all the participating fireflies were assigned their

In the above algorithm, first vector generation function has been mentioned, which has been defined later. Then, each coordinates of all the participating fireflies were assigned. Now, each firefly's fitness function has been checked. Then, until the last iteration has been reached, less brighter fireflies will move towards brighter fireflies followed by fitness checking again.

$\boldsymbol{Algorithm\ 1.1}$: $\boldsymbol{Dual\ Neuro-Genetic\ Vector}()$
$\boldsymbol{Input(s)}$: $Length\ of\ DNGF: N$
$\boldsymbol{Output(s)}$: $Genetic\ Weight\ Vector: Gn$
$Assign\ Epochs1 \leftarrow 0$
$While\ [Counter\ != Maximum\ Epoch]$
Assign $X1_i \leftarrow 1, X_1, X_2, \ldots, X_N$
$WT1[i] = RandomRealNumber(-1, +1)\ /*\ Weight\ Initialization\ */$

$$H1 \leftarrow WT1[Bias] + \sum_{i=1}^{N} WT1_i * X1_i \quad /*\ Hidden\ Output\ */$$

$If\ (H1 <= Desired\ Value) Then$
$Z1_i \leftarrow 0$
$Else$
$Z1_i \leftarrow 1$
$If\ (Z1_i\ != Desired\ Value)\ Then$
$WT1_{Next} = WT1_{Prev} + \{ LR * X1_i \}$
$Bias_{Next} = Bias_{Prev} +$ [LR * Desired Value]
$Else$
$WT1_{Next} = WT1_{Prev}$
$Bias_{Next} = Bias_{Prev}$
$Assign\ Epochs1 \leftarrow Epochs1 + 1$
$End\ while$

$Assign\ Epochs2 \leftarrow 0$
$While\ [Counter\ != Maximum\ Epoch]$
Assign $X2_i \leftarrow 1, X_1, X_2, \ldots, X_N$
$WT2[i] = RandomRealNumber(-1, +1)\ /*\ Weight\ Initialization\ */$

$$H2 \leftarrow WT2[Bias] + \sum_{i=1}^{N} WT2_i * X2_i \quad /*\ Hidden\ Output\ */$$

$If\ (H2 <= Desired\ Value) Then$
$Z2_i \leftarrow 0$
$Else$
$Z2_i \leftarrow 1$
$If\ (Z2_i\ != Desired\ Value) Then$
$WT2_{Next} = WT2_{Prev} + \{ LR * X2_i \}$
$Bias_{Next} = Bias_{Prev} +$ [LR * Desired Value]
$Else$
$WT2_{Next} = WT2_{Prev}$
$Bias_{Next} = Bias_{Prev}$
$Assign\ Epochs2 \leftarrow Epochs2 + 1$
End while

$Itr = 0$
$If[\ Itrn < In]\ Then$
$Mate\_Pool\ [J] \leftarrow TopFit\_Firefly\ [N]$
$J = J + 1$
$Itrn = Itrn + 1$
$End\ if$
$PIVOTAL: R1 = \boldsymbol{Call\ UserRandomFun}()$
$R2 = \boldsymbol{Call\ UserRandomFun}\ ()$
$If\ (R1 == R2)\ Then$
$Go\ to\ Level\ PIVOTAL$
$Else$
$Gn1[\ ], Gn2[\ ] \leftarrow \boldsymbol{CallGeneticCrossOver}(WT1, WT2, R1, R2)$
$End\ if$
$End\ while$

In this above algorithm, double neural machines were installed in each participating terminals of COVID-19 telepsychiatry. Through the neural perceptron protocol, two weight vectors were generated. After that key pool has been desined. Lastly, genetic operation was carried out to have more robust keys.

In this above presented algorithm, it has been designed a random function. This function will return two intermediate values within the length of the key pool. The random number will vary in each of its users.

Algorithm* 1.2: *User Random Function

***Input*(*s*)**: L: $Length\ of\ Chromosome,\quad MS$: $No.of\ Multiple\ Session$

***Output*(*s*)**: $List\ of\ Random\ numbers$

$L = Input\ (\text{“}Enter\ the\ length\ of\ weight\ vector\ \text{”})$
$Assign\ Count = 0$
$While(\ Count\ != MS)$
$R1 = RandomRange(0, +L)$
$R2 = RandomRange(0, +L)$
$If\ (\ R1 != R2)\ Then$
$Assign\ Count = Count + 1$
$End\ if$
$If\ (R1 \geq R2)\ then$
$Set\ T = R1$
$Set\ R1 = R2$
$Set\ R2 = T$
$End\ if$
$End\ while$

Proposed Algorithm 1.1.1: Genetic crossover
Input(s): $Parent\ 1(P1\ [n]), Parent\ 2(P2[n]), Crossover\ Points(\ R1, R2)$
Output(s): $Concatenated\ children, Gn$
$If\ (\ R1 \geq R2)\ then$
$Set\ Temp = R1$
$Set\ R1 = R2$
$Set\ R2 = Temp$
$End\ if$
$Set\ I = 0$
$While\ (\ I < R1)$
$C2[I] = P1[I]$
$C1[I] = P2[I]$
$Set\ I = I + 1$
$End\ while$
$Set\ I = R1 + 1$
$While\ (\ I < (R1 + R2))$
$C2[I] = P2[I]$
$C1[I] = P1[I]$
$Set\ I = I + 1$

$End\ while$
$Set\ I = R2$
$While\ (\ I < n)$
$C2[I] = P1[I]$
$C1[I] = P2[I]$
$Set\ I = I + 1$
$End\ while$
$Gn = C1[n] \,||\, C2[n]$
$Return\ Gn$

In this algorithm mentioned above, genetic crossover was carried out. It has been performed two point crossover on two random points which were obtained through previous algorithm. The child chromosomes will have mixed flavor of both the parents. This would increase our efficacy.

Results and Discussion

In this segment, the outcomes which were seen in the proposed procedure have been briefed here. The processing machine was enabled with the accompanying setups. An i7 Xth Generation (Intel Core), 2.6 GHz CPU processor, 1 TB hard disk, 16 GB primary memory, and so forth. A few numerical-based tests were directed to keep the patients' security and secrecy unblemished. The decimal accuracy of 10^{-15} was considered for those mathematical activities in this procedure, according to the IEEE Standard 754 confirmation. Python was the programming language that has been involved in this strategy. Obviously, there a few purposes behind picking Python here. They are updated library structures, open-source code, portability, easy to make and execute, deciphered language, etc. In the accompanying sub-sections, it has been shown various statistical tests with their adequacy which were done on the proposed DNGF transmission key on COVID-19 2nd wave telepsychiatry.

Dual Neural Genetic Firefly (DNGF) Transmission Key

The accompanying Table 2 has five DNGF transmission keys that were created through this proposed algorithm that

Table 2 Neural Firefly Key Pool

DNGF CODE	DNGF Transmission Keys
DNGF#1	e420ce3a9ccfc8a4
DNGF#2	10b47fd 03a9c8a5
DNGF#3	e2a3c594c35b33d7
DNGF#4	c5403e8002f56821
DNGF#5	2c7bdc9076240f4f

was intended to have the encryption in the E-commerce segment [59]. The patients' medical data has been taken into consideration in COVID-19 telepsychiatry. The engineering of the neural perceptron has been made adaptable and public to all. Be that as it may, the underlying weight vector has not been revealed. The underlying firefly weight vector has been generated through genetic operations. It has been made to fix the malware assignments performed by the intruders. The key robustness of the proposed DNGF transmission key sets has been talked about in later sub-segments.

In the Table 2, it has been presented five proposed DNGF transmission keys having length 128 bits along with their DNGF codes. No symmetricity can be derived between any pair of newly proposed keys. It reflects the dynamic intrusion repulsion capabilities inside COVID-19 s wave of telepsychiatry.

Statistical Test on DNGF

Factual trial of the National Institute of Standard and Technology (NIST 800–22), have been tested on the proposed set of transmission keys which were given in Table 2. Fifteen measurable tests have been endorsed in the NIST test suite to discover the level of irregularity [60]. The goal is to decide the randomized example of pieces disseminated inside the proposed set of DNGF transmission keys. The normal p-values of fifteen such tests have been referenced in the going with Table 3.

From Table 3, it has been found that five proposed DNGF transmission keys have yielded positive p-values in those fifteen statistical tests. Table 3 proves the efficacy of the proposed keys on E-commerce. They can be used for different transaction sessions. We have considered different online sessions for the COVID-19 telepsychiatry. Patients' data can be encrypted through these DNGF keys with efficacy.

DNGF Transmission Key Space

In this proposed technique it has been generated a pool of dual neural-genetic firefly (DNGF) transmission key. They have been formed to have secured data communication in COVID-19 telepsychiatry. Any cryptographic method which has been completely speculatively tried as far as its exhibition should be going through the assault investigation timing [61]. It is expected to investigate the ciphertext that has been scrambled by the proposed DNGF. With the quickest supercomputers, intruders will put their best to translate the session key. The vigor of the transmission key will be tried here. In this proposed strategy, the length of the meeting key is dynamic. To decipher a solitary code text, the quantity of stages on the DNGF is 3.403×10^{38} trial preliminaries. The most recent quickest machine is Japan's Fugaku. It has an execution speed of 415.53 petaflops. The relating time required can be determined under Brute-Force assault with the following Eq. 4.

$$\mathrm{BF(DNGF)} = 2^{L+L}/\left(415.50 * 10^{12}\right) * 3153600 \tag{4}$$

Here, BF (DNGF) is the time for Brute-Force attacks; L denotes the length of DNGF. The following Table 4 will display the approximate time to decode the transmission key on COVID-19 s wave telepsychiatry.

Table 3 Statistical Performance of DNGF Transmission Keys

Serial Number	NIST Name	DNGF#1	DNGF#2	DNGF#3	DNGF#4	DNGF#5
1	Frequency	0.282	0.257	0.346	0.304	0.295
2	Frequency (Block-wise)	0.425	0.407	0.384	0.388	0.429
3	Run	0.332	0.318	0.348	0.287	0.250
4	Longest Run of Ones in Block	0.310	0.348	0.369	0.381	0.367
5	Binary Matrix Run	0.347	0.358	0.391	0.359	0.277
6	Discrete Fourier Transformation	0.229	0.257	0.269	0.277	0.293
7	Non overlapping Template Matching	0.301	0.354	0.357	0.344	0.372
8	Overlapping Template Matching	0.281	0.396	0.251	0.256	0.363
9	Maurer's Universal Statistical	0.347	0.343	0.315	0.269	0.454
10	Linear Complexity	0.436	0.377	0.369	0.422	0.471
11	Serial	0.236	0.307	0.410	0.328	0.418
12	Approximate Entropy	0.246	0.287	0.296	0.314	0.268
13	Cumulative Sum	0.302	0.487	0.344	0.296	0.309
14	Random Excursion	0.457	0.467	0.308	0.258	0.328
15	Random Excursion Variant	0.388	0.294	0.231	0.285	0.360

In Table 4, it has been computed the time needed to decode the proposed DNGF key. For key length 14 bits, 56 bits, and 128 bits, $2.04*10^{11}$ years, $2.59*10^{15}$ years, and $8.83*10^{57}$ years will be needed respectively.

Graphical Analysis

Mindfulness and protections are simply the most ideal approaches to protect from this perilous coronavirus [62]. Here, two kinds of graphical investigation were done on the proposed DNGF transmission keys. They are histogram and autocorrelation experiment. The adequacy of the outcomes can show an effective mechanism for COVID-19 telepsychiatry. This demonstrates the vigor of the proposed E-commerce procedure in this worldwide crown pandemic. This proposed strategy on heterogeneous information can shield the various sorts of assaults [63].

Histogram Experiment

The clinical signal online database has been used in this study for the proposed RSKs to establish its efficiency and effectiveness [64]. Histogram analysis has been carried out at this proposed technique. How binary values of 1 s and 0 s of a plain signal are spread, this has been studied. A graphical representation of frequency distribution inside the signals has been studied. The distribution of data i.e. peaks; spreads and symmetricity is not relevant. The peaks bars represent the maximum occurrences and spreads represent the information variation. This technique is valid in COVID-19 wireless telemedicine systems. The proposed key generation scheme may be accomplished as a session key of COVID-19 wireless telemedicine. The efficacy in terms of histogram has been shown in Fig. 5.

To set up the proficiency and adequacy of the proposed DNGF transmission key, histogram experiment has been performed [64]. How double upsides of 1 and 0 s of a plain sign are spread, this has been contemplated here. A graphical portrayal of recurrence circulation inside the signs has been contemplated. The dispersion of information for example tops; spreads and symmetricity isn't important. The pinnacles bars address the most extreme events and spread address the data variety. This procedure is substantial in COVID-19 telepsychiatry where a patient can communicate in a safe way. The proposed key generation plan might be refined as a transmission key of COVID-19 s wave telepsychiatry. The efficacy as far as histogram has been appeared in the accompanying Fig. 3.

Table 4 DNGF Transmission Key Space–Time

Sl. No	Size of DNGF Key	Time needed(in years)
1	14 bits	$2.04*10^{11}$
2	56 bits	$2.59*10^{15}$
3	128 bits	$8.83*10^{57}$

Autocorrelation Experiment

Investigation of autocorrelation on the proposed DNGF transmission key has been acted in this sub-segment. Autocorrelation of a plain text is a similitude record at various points. Autocorrelation of the plain text won't be reasonable for any encryption. Also, the viability as far as autocorrelation has been introduced in the accompanying Fig. 4.

In Fig. 4, autocorrelation graph has been spread uniformly while using the proposed DNGF transmission key. It adds the efficacy of the proposed technique.

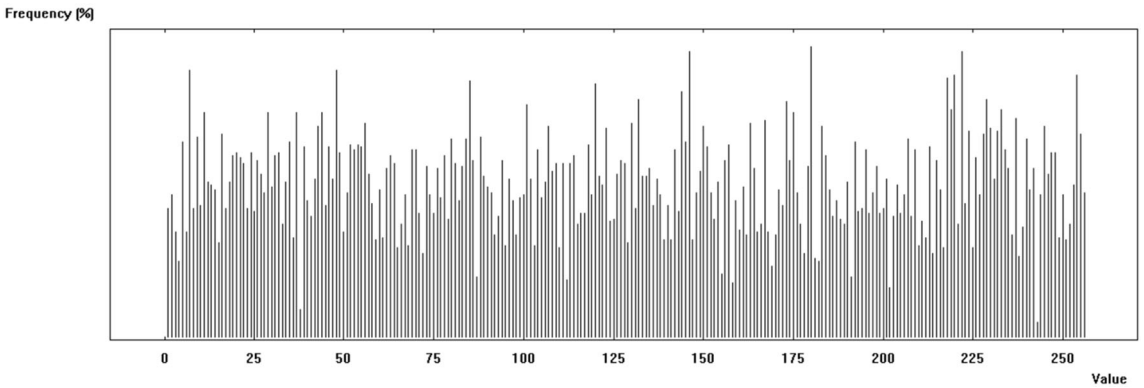

Fig. 3 Histogram on proposed DNGF Transmission Key

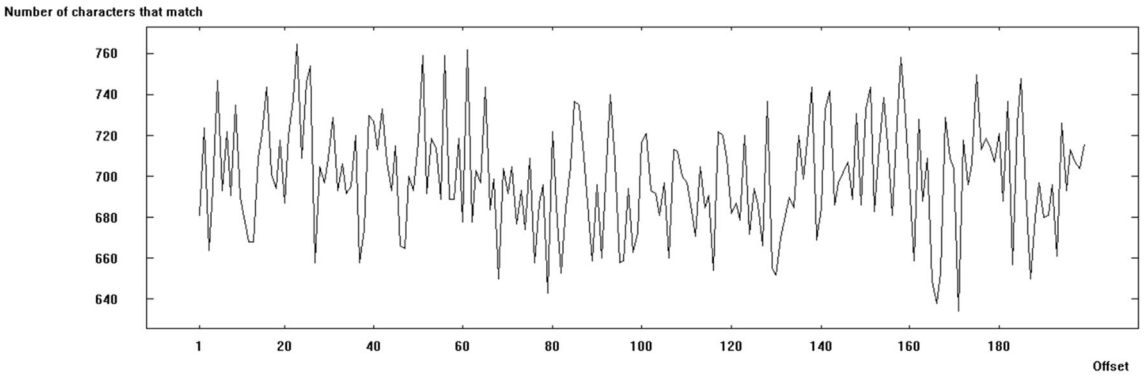

Fig. 4 Autocorrelation on proposed DNGF Transmission Key

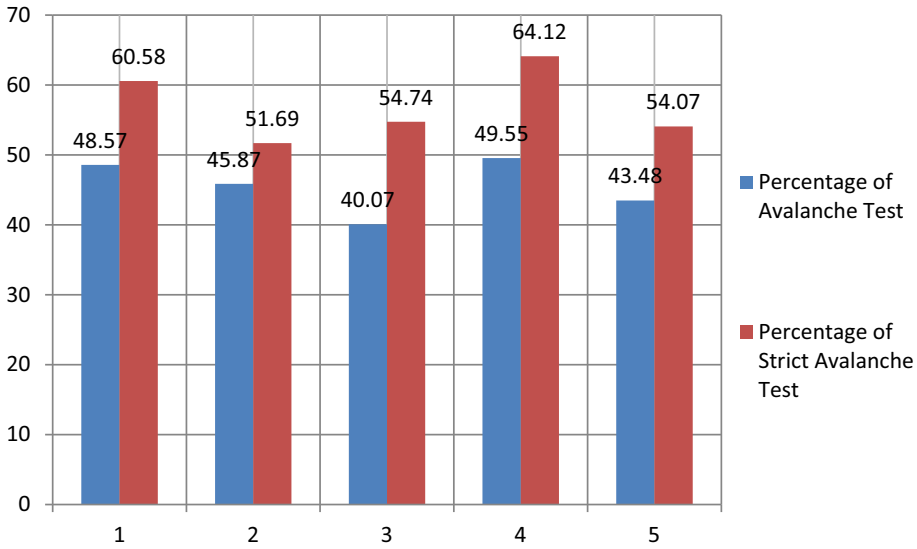

Fig. 5 Percentage of Avalanche & Strict Avalanche Test on DNGF

DNGF Performance using Avalanche and Strict Avalanche Test

The performance of the proposed DNGF transmission keys with Avalanche Test has been tried to find out in this work along with the Strict Avalanche Test. In any encryption method, it is viewed as another critical angle to distinguish the Man-In-The-Middle attacks. Avalanche test has been done to distinguish the changed impact in the ciphertext. That implies minor adjusted pieces of the plain text would acquire extraordinary changes the proposed figure text with the help of same DNGF. In Strict Avalanche test, the level of adjustments should be bigger than half of the pieces in the proposed figure text [65]. Here, the proposed DNGF on COVID-19 telepsychiatry has been tried under these two trials on similar plain data. The normal percentage of changes while leading the said tests has been noted in the accompanying Fig. 5.

In Fig. 5, it has been analyzed Avalanche and Strict Avalanche effect on the proposed set of Dual Neural Genetic Firefly (DNGF) transmission key. It is clearly visible that it had passed both the statistical tests with positive outcomes.

Functional Security Parameter

It has been examined the functional security viability of the proposed DNGF transmission key on COVID-19 2nd wave of telepsychiatry. The capacity that has been proposed to characterize the functional security issue has been founded on the proposed transmission key. It has been characterized in the accompanying Eq. 5.

$$\text{FSP} = f(\text{DNGF}, \text{Statistical Test}) \tag{5}$$

Here, FSP is the functional security parameter, DNGF is the individual proposed transmission key, and Statistical Test is the mean outcome of NIST. Effectively in the

Table 5 Functional Security Parameters outcome

DNGF CODE	Functional Security Parameter (FSP) Outcome
DNGF#1	0.327933
DNGF#2	0.350467
DNGF#3	0.332533
DNGF#4	0.317867
DNGF#5	0.350267

earlier sub-areas, the effectiveness of DNGF in measurable statistical tests has been referenced. Utilizing the above-proposed work, the functional security parameter can be estimated in this COVID-19 telepsychiatry. It has been summed up in the accompanying Table 5.

In the above specified Table 5, the noted FSP value for five DNGF keys are 0.327933, 0.350467, 0.332533, 0.317867, and 0.350267. All such values were at par excellence.

DNGF Transmission Key Security Analysis

In any E-commerce segment, the data transmission security must be strong enough to resist intruders. In this work, it has been proposed a set of DNGF transmission keys on COVID-19 telepsychiatry. Following are the security aspects that were emphasized and analyzed during this transmission key generation.

- Patients' Data confidentiality: Patients' data confidentiality is the most relevant issue that needs highest attention in any telemedicine. Keeping the same track, it has been designed a set of DNGF transmission key, and those were tested under various experiments likes of statistical tests, functional security, graphical analysis, etc.
- Session Key Distribution: In most of cases, the session is being publicly distributed to the patient and doctor. There exists a maximum chance of trapping those keys by the opponents. So there must be a secured mechanism for its distribution.
- Patients' Data integrity: On the off chance that the patients' data packets are gotten by encryption methods and secured session keys. The enemies can't have the option to peruse or take information yet at the transmission time. It can add some false information or any perilous content with information in the psychiatric treatment procedure. Accordingly, information honesty ensures that any got information has not changed during transmission period.
- Data freshness: As the patients' data honesty has significance in information security and adds a comparable newness in the digital telehealth network correspondence. The cryptographic keys should be invigorates, recharge, and changed with respect to time. The information newness can ready to forestall a replay assault. Timestamps can be utilized to address these issues. In this regard, it has been proposed the multiple set of DNGF transmission keys.
- Self-organization of the telepsychiatry network: A COVID-19 telepsychiatry network has been proposed as self-organized here. Dual neural networks were participated to generate the weight vector. The symmetry of both the networks is same and kept hidden the seed values. It has been done to protect against the threats of opponents.
- Secured localization of terminals: An adversary can easily retrieve the patients' data if the terminal is compromised. So secured localization of the terminals at the patients' end and psychiatrists' end is mandatory. That's why robust DNGF transmission key pool has been developed.
- Accountability: Responsibility necessitates that the conduct of an individual patient should be ascribed exclusively to that element of COVID-19 telepsychiatry. It is getting the basic issues like non-repudiation, fault seclusion, intrusion detection, and legitimate activities. In this regard, further biometric keys may be attached as protocol sub-domain.
- System Survival: Every E-commerce system has its own survival potency. It includes malware prevention, data secrecy, risk handling, recovery activities, etc. The survival of the proposed COVID-19 telepsychiatry is good in terms of the mathematical tests conducted on DNGF transmission keys.

Time needed in DNGF Generation

It is a very evident parameter that the time needed to generate the proposed DNGF should be less. Any cryptographic scheme needs a secret key to dwell with the encryption standards. In Table 6, the time needed in this regard has been noted carefully.

Table 6 has the following table headers as DNGF CODE, and Generation Time (in ms). The correlation coefficient between the generation time and their functional security parameters has been found to be $r_{GT,FS} = -0.53404$. Thus, it can be stated that there exists no correlation between them.

Table 6 Time Needed in DNGF Formation

DNGF CODE	Generation time (in ms)
DNGF#1	719.57
DNGF#2	691.07
DNGF#3	665.21
DNGF#4	701.94
DNGF#5	663.11

Time Complexity of DNGF

The proposed method of session key generation has been splitted into four sub-modules. They are Neural weight generation, Genetic operation, Firefly algorithm, and DNGF transmission key generation. In Table 7, it has been calculated the time complexity of the said modules.

Since in the proposed neural network, the weight vector was created with N and K number of input and hidden neurons, hence the order of its complexity can be of $O(N * K)$. The genetic operation pours extra robustness to the proposed key. Its complexity may be of the order of $O(L)$ with L being the size of the parent chromosome. The proposed firefly algorithm has the complexity of the order of $O(N)$ having N number of fireflies. Lastly, the module of Dual Neural Genetic Firefly (DNGF) transmission key has been associated with complexity $O(N)$ with N numbered fireflies participating in the algorithm.

Comparison with Earlier Works

It has been described in this work a tabular structure to have a comparison between the proposed DNGF and earlier works. The following Table 8 has shown the valued comparisons with its needs.

Table 7 Time Complexity Generation

Sl. No	Sub-modules	Time Complexity	Parameter(s) name
1	Neural weight generation	$O(N * K)$	$N =$ No.of input neurons, $K =$ No. of hidden neurons
2	Genetic operation	$O(L)$	$L =$ Length of parent chromosome
3	Firefly algorithm	$O(N)$	$N =$ No. of fireflies
4	DNGF transmission key generation	$O(N)$	$N =$ No. of fireflies

Table 8 Comparison with previous works

Sl. No	Properties of Comparison	Essence of such properties	Ref No. 68	Ref No. 69	Ref No. 70	Ref No. 71	Ref No. 72	Proposed technique
1	E-Commerce Segment Focus	COVID has immensely triggered the E-commerce	No	No	No	No	No	Yes
2	Telepsychiatry	Very much relevant on COVID-19 2nd wave	No	No	No	No	No	Yes
3	Patients' Data Sensing in live mode	It is important to monitor the patients' data in online continuous mode	No	No	No	No	No	No
4	Data Encryption/Session Key generation	Cryptography deals with strong encryption method with session key	Yes	Yes	Yes	Yes	Yes	Yes
5	Patients' Data Compression	To curtail the size of the cipher text	No	No	Yes	No	No	No
6	Analysis on Session Key Space	Time needed to decipher the Session Key	No	No	No	No	Yes	Yes
7	Histogram graph	To check the distribution of characters	No	No	No	No	Yes	Yes
8	Autocorrelation graph	Whether there exists any similarity between a ciphertext pattern and its plain version?	Yes	No	No	No	Yes	Yes
9	Key generation time	It is used to find the key generation time	No	Yes	No	No	Yes	Yes
10	Statistical NIST	Randomness checking inside the keys	No	No	No	No	Yes	Yes
11	Avalanche Effect	To detect the modifications in the ciphertext	No	No	No	No	No	Yes
12	Strict Avalanche Effect	To detect the more than 50% of modifications in the ciphertext	No	No	No	No	No	Yes
13	Comparative Statement	To summarize the comparison work	No	No	No	No	Yes	Yes

Table 9 Gap Analysis with earlier papers

Sl. No	Earlier papers	Positive outcome(s)	Limitation(s)	Proposed technique addressed those limitation(s)
1	O'Brien et al. [32]	Implementation of telepsychiatry during COVID-19 period	No security mechanism	Telepsychiatry data has been protected against vulnerabilities
2	Bokolo [33]	Usage of virtual care through telemedicine	Data protection was absent	Efficient session key was proposed as DNGF transmission key
3	Stoll et al. [35]	Ethical use of telepsychiatry was done	Privacy has not been addressed	Patients' data privacy has been focused through higher cryptosystem
4	Rezaeibagha et al. [37]	Users' mobility with respect to telemedicine has been emphasized	System Complexity was not found	Complexity has been calculated here
5	Chao et al. [39]	Use of metaheuristic firefly algorithm to train the images	Key robustness was missing	Robustness of the proposed set of keys was checked
6	Rani et al. [45]	Medical images were compressed using firefly algorithm	Security analysis was not conducted here	Security analysis was performed on the private data
7	Alomoush et al. [48]	Automatic image segmentation based fuzzy C-means with firefly algorithm was present	Time needed was not calculated	Time needed has been shown

Gap Analysis

It has been cited the positive and negative outcomes of some of the literature section papers. Moreover, it has also been noted how the proposed technique has dealt to address those negative outcomes. In Table 9, it has been clearly mentioned the said things in brief.

Conclusions

With the spikes in the COVID-19 positive graphs during the second wave, remote telepsychiatry is the best option to treat the patients' mental illness. It is also very much equally important to treat the COVID-19 patients under COVID-19 treatment rules along with psychiatric treatments. Despite the fact that patients' information protection is a fundamental matter of concern. Cryptographic designing on the clinical information is the most suitable approach to guarantee patients' classification [71, 72]. The volume of E-business exchanges had sped up in a gigantic scope because of COVID-19 spikes. Telepsychiatry goes under the section of E-commerce, where the patients can get their mental illness treatments from the disconnects. Patients' data security is a fundamental test in this COVID-19 telepsychiatry. Online commercial transactions have immensely burdened online open network activities. In order to counter-attack the intruding, it is needed to generate a strong transmission key pool as proposed DNGF transmission key. With such proposed keys, patients' medical data can be encrypted in public correspondence. In this paper, the pool of transmission keys was generated with the help of firefly algorithm, double neural perceptrons, and genetic crossover. It has effectively passed Avalanche test and Strict Avalanche test. The output of the proposed Functional Security Parameter (FSP) test has been noted as 0.327933, 0.350467, 0.332533, 0.317867, and 0.350267 on the proposed pool of DNGF. The time needed for the proposed DNGF pool generation has been observed as 719.57 ms, 691.07, 665.21, 701.94 and 663.11 ms. The correlation coefficient between the key generation time and Functional Security Parameter (FSP) has been calculated as $r_{GT,FS} = -0.53404$. It has shown better reasonability on the part of the COVID-19 2nd wave telepsychiatry, which is a major component of E-commerce.

Limitations and Future Scope of Work

The limitation of this DNGF transmission key generation is that the architecture of two neural networks should be unique. Another limitation was that the difference between two random crossover points could be minimum which provides fewer blends in the concatenated child vector. It means when the modular difference between two crossover points is small, then it leads to minor shuffling inside the resultant vector.

In future, this technique can be modified to work on different metaheuristic algorithms likes of salp swarm, honey bee, etc. Use of different other techniques could result in more robust transmission keys. Moreover, automated authentication of the patients and the psychiatrist is tremendously recommended as its future scope of work.

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

Funding No research fund has been received.

Declarations

Conflict of interest On behalf of all authors, the corresponding author states that there is no conflict of interest.

References

1. B. Anthony, Use of telemedicine and virtual care for remote treatment in response to COVID-19 pandemic. J. Med. Syst. **44**, 132 (2020). https://doi.org/10.1007/s10916-020-01596-5
2. K. Okereafor, O. Adebola, R. Djehaiche, Exploring the potentials of telemedicine and other non-contact electronic health technologies in controlling the spread of the novel coronavirus disease (COVID-19). IJITE. **8**(4), 1–13 (2020)
3. Hollander JE, Carr BG. Virtually perfect? Telemedicine for COVID-19. N Engl J Med 2020.
4. J. Dey, S. Mukherjee, Wireless COVID-19 telehealth: leukocytes encryption guided by amino acid matrix. Wirel. Pers. Commun. (2021). https://doi.org/10.1007/s11277-021-08534-9
5. A.J. Bokolo, Exploring the adoption of telemedicine and virtual software for care of outpatients during and after COVID-19 pandemic. Ir. J. Med. Sci. **2020**, 1–10 (1971)
6. Kadir, M. A. (2020). Role of telemedicine in healthcare during COVID-19 pandemic in developing countries. Telehealth and Medicine Today. https://doi.org/10.30953/tmt.v5.187
7. W.A. Khan, N.N. Hamadneh, S.L. Tilahun, J.M.T. Ngnotchouye, A review and comparative study of firefly algorithm and its modified versions. Optim. Algorithms-Methods Appl, Ozgur Baskan, IntechOpen, (2016). https://doi.org/10.5772/62472
8. J. Dey, Pivotal "New Normal" Telemedicine: secured psychiatric homeopathy medicine transmission in Post-COVID. Int. j. inf. tecnol. (2021). https://doi.org/10.1007/s41870-021-00675-1
9. World Health Organization (WHO) Coronavirus disease (COVID-19): weekly operational update on COVID-19 (2020). https://covid19.who.int/. Accessed on 25 May 2021.
10. Information Accessed on 25 May 2021 from: https://www.covid19india.org/
11. Pierce BS, Perrin PB, Tyler CM, McKee GB, Watson JD. (2020) The COVID-19 telepsychology revolution: a national study of pandemic-based changes in U.S. mental health care delivery [published online ahead of print, 2020 Aug 20]. Am Psychol. https://doi.org/10.1037/amp0000722
12. J. Torous, K. Jän Myrick, N. Rauseo-Ricupero, J. Firth, Digital mental health and COVID-19: using technology today to accelerate the curve on access and quality tomorrow. JMIR Mental Health **7**(3), e18848 (2020). https://doi.org/10.2196/18848
13. J.H. Wright, R. Caudill, Remote treatment delivery in response to the COVID-19 pandemic. Psychother. Psychosom. **89**(3), 130–132 (2020). https://doi.org/10.1159/000507376
14. H. Mahmoud, E. Whaibeh, B. Mitchell, Ensuring successful telepsychiatry program implementation: critical components and considerations. Curr. Treat. Options Psychiatr. **7**(2), 186–197 (2020). https://doi.org/10.1007/s40501-020-00208-w
15. E. Whaibeh, H. Mahmoud, H. Naal, Telemental health in the context of a pandemic: the COVID-19 experience. Curr. Treat. Options Psychiatr. **7**, 1–5 (2020). https://doi.org/10.1007/s40501-020-00210-2
16. Y.S. Hau, J.K. Kim, J. Hur, M.C. Chang, How about actively using telemedicine during the COVID-19 pandemic? J. Med. Syst. **44**, 1–2 (2020)
17. K. Hariss, H. Noura, A.E. Samhat, An efficient fully homomorphic symmetric encryption algorithm. Multimed. Tools Appl. **79**, 12139–12164 (2020). https://doi.org/10.1007/s11042-019-08511-2
18. E.A. Kadhim, Z.K. Hussein, H.J. Hadi, AES cryptography algorithm based on intelligent Blum–Blum–Shub PRNGs. J. Eng. Appl. Sci. **12**, 9035–9040 (2017)
19. W. Stallings, Cryptography and Network Security: Principles and Practice, third edition, Prentice Hall, 2003.
20. Bhowmik A., Karforma S., Dey J., Sarkar A. (2020), *Fuzzy-Based Session Key as Restorative Power of Symmetric Key Encryption for Secured Wireless Communication*. In: Kundu S., Acharya U., De C., Mukherjee S. (eds) Proceedings of the 2nd International Conference on Communication, Devices and Computing. Lecture Notes in Electrical Engineering, vol 602. Springer, Singapore.
21. A. Agrawal, S. Gorbunov, V. Vaikuntanathan, H. Wee, Functional encryption: New perspectives and lower bounds, in R. Canetti, J.A. Garay, (eds.) CRYPTO 2013, Part II. LNCS, vol. 8043. (Springer, Heidelberg, 2013), pp. 500–518.
22. D. Stinson, Cryptography: Theory and Practice, third edition, Chapman & Hall/CRC, 2006.
23. H.N. Khan, A. Chaudhuri, A. Das et al., An ultra robust session key based image cryptography. Microsyst Technol **26**, 2193–2201 (2020). https://doi.org/10.1007/s00542-019-04518-9
24. Tharakan L.A., Daniel S., Dhanasekaran R. (2021) Security Enhancement and Monitoring for Data Sensing Networks Using a Novel Asymmetric Mirror-Key Data Encryption Method. In: Malik H., Fatema N., Alzubi J.A. (eds) AI and Machine Learning Paradigms for Health Monitoring System. Studies in Big Data, vol 86. Springer, Singapore.
25. O. Reyad, M.E. Karar, Secure CT-image encryption for Covid-19 infections using hbbs-based multiple key-streams. Arab J Sci Eng **46**, 3581–3593 (2021). https://doi.org/10.1007/s13369-020-05196-w
26. A.K. Gautam, R. Kumar, A comprehensive study on key management, authentication and trust management techniques in wireless sensor networks. SN Appl. Sci. **3**, 50 (2021). https://doi.org/10.1007/s42452-020-04089-9
27. M. Mitev, A. Chorti, M. Reed et al., Authenticated secret key generation in delay-constrained wireless systems. J. Wirel. Commun. Netw. **2020**, 122 (2020). https://doi.org/10.1186/s13638-020-01742-0
28. R.S. Goswami, S.K. Chakraborty, A. Bhunia et al., New techniques for generating of automatic variable key in achieving perfect security. J. Inst. Eng. India Ser. B **95**, 197–201 (2014). https://doi.org/10.1007/s40031-014-0103-2
29. A. Sarkar, J. Dey, A. Bhowmik, S.S. Ferdows, A dynamic key generation scheme based on Metaheuristic cuckoo search. Int. J. Comput. Sci. Eng. **07**(01), 184–187 (2019)
30. 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.
31. E. Monaghesh, A. Hajizadeh, The role of telehealth during COVID 19–19 outbreak: a systematic review based on current evidence. BMC Public Health **20**, 1193 (2020). https://doi.org/10.1186/s12889-020-09301-4
32. M. O'Brien, F. McNicholas, The use of telepsychiatry during COVID 19–19 and beyond. Ir. J. Psychol. Med. **21**, 1–6 (2020)
33. B. Anthony, Use of telemedicine and virtual care for remote treatment in response to COVID 19–19 pandemic. J. Med. Syst. **44**, 132 (2020). https://doi.org/10.1007/s10916-020-01596

34. M. Gautam, A. Thakrar, E. Akinyemi, G. Mahr, Current and future challenges in the delivery of mental healthcare during COVID 19–19. SN Compr. Clin. Med. **11**, 1–6 (2020). https://doi.org/10.1007/s42399-020-00348-3
35. J. Stoll, J.Z. Sadler, M. Trachsel, The Ethical Use of Telepsychiatry in the COVID 19–19 Pandemic. Front. Psychiatr. **11**, 665 (2020). https://doi.org/10.3389/fpsyt.2020.00665
36. K. Smith, E. Ostinelli, O. Macdonald, A. Cipriani, COVID 19–19 and telepsychiatry development of evidence-based guidance for clinicians. JMIR Ment. Health **7**(8), e21108 (2020). https://doi.org/10.2196/21108
37. F. Rezaeibagha, Yi Mu, Practical and secure telemedicine systems for user mobility. J. Biomed. Inform. **78**, 24–32 (2018)
38. X.-S. Yang, Firefly algorithm, stochastic test functions and design optimisation. Int. J. Bio-Inspired Comput. **2**(2), 78–84 (2010)
39. C.-F. Chao, M. Horng, Firefly algorithm for training the radial basis function network in ultrasonic supraspinatus image classification. Comput. Model New Technol. **18**(3), 77–83 (2014)
40. T. Apostolopoulos, A. Vlachos, Application of the firefly algorithm for solving the economic emissions load dispatch problem. Int. J. Combinator. **2011**, 523806 (2010)
41. Jati G.K., Suyanto (2011) Evolutionary discrete firefly algorithm for travelling salesman problem. In: Bouchachia A. (eds) Adaptive and Intelligent Systems. ICAIS 2011. Lecture Notes in Computer Science, vol 6943. Springer, Berlin, Heidelberg.
42. S. Karthikeyan et al., A hybrid discrete firefly algorithm for solving multi-objective flexible job shop scheduling problems. Int. J. Bio-Inspired Comput. **7**(6), 386–401 (2015)
43. J. Senthilnath, S.N. Omkar, V. Mani, Clustering using firefly algorithm: performance study. Swarm Evolution Comput. **1**(3), 164–171 (2011)
44. Veeramuthu A, Meenakshi S. Breeding firefly association rules for effective medical image retrieval. Biomed. Res. Artif. Intell. Tech. Bio. Med. Signal Process. 2017.
45. M.L.P. Rani, G.S. Rao, B.P. Rao, An efficient codebook generation using firefly algorithm for optimum medical image compression. J. Ambient Intell. Human Comput. **12**, 4067–4079 (2021). https://doi.org/10.1007/s12652-020-01782-w
46. M.H. Ab Talib, I.Z. Mat Darus, P. Mohd Samin et al., Vibration control of semi-active suspension system using PID controller with advanced firefly algorithm and particle swarm optimization. J. Ambient Intell. Human Comput. **12**, 1119–1137 (2021). https://doi.org/10.1007/s12652-020-02158-w
47. B. Fan, W. Yang, Z. Zhang, Solving the two-stage hybrid flow shop scheduling problem based on mutant firefly algorithm. J. Ambient Intell. Human Comput. **10**, 979–990 (2019). https://doi.org/10.1007/s12652-018-0903-3
48. W. Alomoush, A. Alrosan, Y.M. Alomari et al., Fully automatic grayscale image segmentation based fuzzy C-means with firefly mate algorithm. J. Ambient Intell. Human Comput. (2021). https://doi.org/10.1007/s12652-021-03430-3
49. M. Anuradha, V. Ganesan, S. Oliver et al., Hybrid firefly with differential evolution algorithm for multi agent system using clustering based personalization. J. Ambient Intell. Human Comput. **12**, 5797–5806 (2021). https://doi.org/10.1007/s12652-020-02120-w
50. C. Vinothini, P. Balasubramanie, Meta-heuristic firefly approach to multi-servers load balancing with independent and dependent server availability consideration. J. Ambient Intell. Human Comput. **12**, 5443–5455 (2021). https://doi.org/10.1007/s12652-020-02032-9
51. S. Meena, K. Chitra, An approach of firefly algorithm with modified brightness for PID and I-PD controllers of SISO systems. J. Ambient Intell. Human Comput. (2018). https://doi.org/10.1007/s12652-018-0747-x
52. N.L. Shah, J.B. Miller, M. Bilal et al., Smartphone apps in graduate medical education virtual recruitment during the COVID-19 pandemic. J. Med. Syst. **45**, 36 (2021). https://doi.org/10.1007/s10916-021-01720-z
53. J. Furmaga, S.A. McDonald, Impact of rapid medical evaluation on patient flow in an urban emergency department. J. Med. Syst. **45**, 63 (2021)
54. R. Cau, P. P. Bassareo, L. Mannelli, J. S. Suri, L. Saba, Imaging in Covid-19-related myocardial injury, Int. J. Cardiovasc. Imag. (2020) 1–12.
55. J. O'Herrin, N. Fost, K. Kudsk, Health insurance portability accountability act (HIPAA) regulations: Effect on medical record research. Ann. Surg. **239**(6), 772–776 (2004). (**discussion 776–778**)
56. J.J. Shen, L.F. Samson, E.L. Washington et al., Barriers of HIPAA regulation to implementation of health services research. J. Med. Syst. **30**, 65–69 (2006). https://doi.org/10.1007/s10916-006-7406-z
57. X.S. Yang, *Nature-inspired meta-heuristic algorithms* (Luniver Press, Beckington, UK, 2008)
58. S. Lukasik and S. Zak, "Firefly algorithm for con-tinuous constrained optimization tasks," in *Proceedings of the International Conference on Computer and Computational Intelligence (ICCCI '09)*, N. T. Nguyen, R. Kowalczyk, and S.-M. Chen, Eds., vol. 5796 of *LNAI*, pp. 97–106, Springer, Wroclaw, Poland, October 2009.
59. A. Bhowmik, S. Karforma, Linear feedback shift register and integer theory: a state-of-art approach in security issues over e-commerce. Electron Commer Res (2021). https://doi.org/10.1007/s10660-021-09477-w
60. Rukhin, A., Soto, J., Nechvatal, J., Smid, M., Barker, E., Leigh, S., Levenson, M., Vangel, M., Banks, D., Heckert, A., Dray, J., and Vo, S.: A statistical test suite for random and pseudorandom number generators for cryptographic applications. NIST special publication 800–22, 2001.
61. A. Sarkar, J. Dey, M. Chatterjee, A. Bhowmik, S. Karforma, Neural soft computing based secured transmission of intraoral gingivitis image in E-health. Indones. J. Electr. Eng. Comput. Sci. **14**(1), 178–184 (2019)
62. J. Dey, S.S. Ferdows, An online social awareness spread to combat recent outbreak of coronavirus. Int. J. Sci. Res. Multidiscip. Stud. **6**(5), 9–14 (2020)
63. J. Dey, A. Sarkar, S. Karforma, Newer post-COVID perspective: Teledental encryption by de-multiplexed perceptrons. Int. J. Inf. Technol. **13**, 593–601 (2021). https://doi.org/10.1007/s41870-020-00562-1
64. Sarkar A., Dey J., Bhowmik A., Mandal J.K., Karforma S., 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.
65. L. Min, G. Chen, A novel stream encryption scheme with avalanche effect. Eur. Phys. J. B **86**, 459 (2013). https://doi.org/10.1140/epjb/e2013-40199-7
66. Ahmad, M., Farooq, O., Datta, S., and Sohail, S. S., Vyas A. L., and Mulvaney D.In: *4th International Conference on Biomedical Engineering and Informatics, 1471–1475*, 2011.
67. C.-F. Lin, S.-H. Shih, J.-D. Zhu, Chaos based encryption system for encrypting electroencephalogram signals. J. Med. Syst. **38**(5), 1–10 (2014)
68. M. Raeiatibanadkooki, S.R. Quchani, M. KhalilZade, K. Bahaadinbeigy, Compression and encryption of ECG sig-nal using wavelet and chaotically huffman code in telemedicine application. J. Med. Syst. **40**(3), 1–8 (2016)

69. C.-F. Lin, Chaotic visual cryptosystem using empirical mode decomposition algorithm for clinical EEG signals. J. Med. Syst. **40**(3), 1–10 (2016)
70. M.A. Murillo-Escobar et al., A double chaotic layer encryption algorithm for clinical signals in telemedicine. J. Med. Syst. **41**, 59 (2017)
71. J. Dey, S. Karforma, A. Sarkar, A. Bhowmik, Metaheuristic guided secured transmission of E-prescription of dental disease. Int. J. Comput. Sci. Eng. **07**(01), 179–183 (2019)
72. A. Sarkar, J. Dey, S. Karforma, Musically modified substitution-box for clinical signals ciphering in wireless telecare medical communicating systems Wirel. Pers. Commun. **117**(727), 745 (2021). https://doi.org/10.1007/s11277-020-07894-y