International Journal of Reconfigurable and Embedded Systems (IJRES)
Vol. 11, No. 1, March 2022, pp. 13~24
ISSN: 2089-4864, DOI: 10.11591/ijres.v11.i1.pp13-24

COVID-19 paediatric cavity telecare system: a novel chain key generation and encryption scheme

Joydeep Dey
Department of Computer Science, Maharajadhiraj Uday Chand (M.U.C.) Women's College, Burdwan, India

Article Info

Article history:

Received Oct 18, 2021
Revised Nov 6, 2021
Accepted Jan 27, 2022

Keywords:

Graphical analysis
Novel chain key generation
Paediatric cavity
Reversible binary image
Telecare information system

ABSTRACT

In this unprecedented coronavirus crisis, telehealth had emerged as a substitute way of treatment. More specifically, paediatric children are at high risk of outside exposure now. Non critical children must be treated remotely through the tableware system. A key based secured online transmission of an intraoral image of the paediatric cavity has been proposed in this manuscript. A cavity is a dental disease occurring in children. It is mainly caused due to prolonged bacterial infections. Secured online transmission with respect to medical transactions is immensely required in telecare information systems (TIS). Data confidentiality factor is preserved with preference in this proposed technique. A parity based novel chain key (NCK) has been generated and diffused inside the intraoral paediatric cavity image. NCK generation scheme is so highly robust that it gives different combinations after each bit altering. Initial seeds are kept at the dentist and patients, to resist myriad attacks inside the wireless channel, especially during this COVID-19 period. Histogram, floating frequency, and autocorrelation were obtained with accuracy using the proposed technique. Effects were observed by flipping simultaneous bits of the initial key and results were highly acceptable. The time for the proposed key generation has been found to be 514.61 ms. The total cryptographic time has been noted as 3.5983 ms in this technique.

Corresponding Author:

Joydeep Dey
Head, Department of Computer Science, M.U.C. Women's College
B.C. Road, Uttar Fatak, Post Rajbati, Burdwan, West Bengal, India
Email: joydeepmcabu@gmail.com

1. INTRODUCTION

Telecare information system (TIS) is a necessary weapon in this era of digital computing. It has become an alternative option to treat the patients from their homes in the time of COVID-19. Thus, the patients and children are not at all exposed to the risk of coronavirus transmission. With the interfaces of such systems, patients can easily communicate with their physicians at any time. Thus, visiting the hospitals/clinics physically has been brought into less frequency. There are so many advantages of using such a TIS. But the biggest thing of concern is security on the medical data [1]–[3]. The chief objective of this manuscript is to a have robust cryptographic system with a strong session key such that it can easily beat the man-in-the-middle attacks inside the telehealth networks. This proposed technique has shown a way to transmit paediatric information by reversible computing structures on dental issues during the COVID-19 era. Dental hygiene care is a cornerstone area of concern that needs pretty good care for children's welfare. Parents are the best care givers to their off springs. The oral health care of a child revolves around the Paediatricians, Paediatric Dentists, Pathologists, Dieticians and Anaesthesiologists. The decay in the tooth is mainly caused due to a group of germs known as *mutans streptococcus and lactobacillus.* The bacterial invasions are raised by the sugar, which then produces acids. The structure of teeth bifurcates by depleting the calcium layer with rising in the potential of hydrogen (pH) levels inside the child's periodontium zone. A plaque created by the bacteria. A yellowish film developed on the buccal surface caused by the enamel eroding acids. De- calcified surface of the teeth collapsed, and thus cavity is being created.

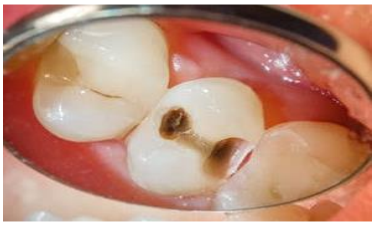

Figure 1. Intraoral image revealing molar cavity

Cryptography is concerned mainly to protect the data from myriad malicious attackers [4]. They distort and manipulate the data and signals while transmission. In cryptography, two keys are public and private key [5], [6]. In TIS too, there has been a tremendous amount of emphasis given on medical data security. Intelligent computing [7] plays a big role in such online health services domains. To ensure integrated data transmission between the nodes is the prime objective in data security [8], [9].

The motivation behind developing this unique novel chain key (NCK) based encryption is to enhance the remote medical assistance to the children in these critical corona times. Due to lockdown restraints, most of the treatments are recommended to be done in virtual modes from secludes. This decreases the coronavirus transmission to the children. It provides immense motivation for design such COVID-19 paediatric cavity telecare system. This paper presents a secured novel technique that generates a Hamming key based on parity information. The binary intraoral image is converted into reversible a Fredkin image. The resultant Hamming key will be diffused with the binary Fredkin image.

The highest concerning issue was the children's data security. During the public communication over the telehealth network, such sensitive data may be hijacked by the silent intruders living in the networks. They will collect those data and manipulate them as per wrong intentions. Data confidentiality and integrity are the most relevant challenges in the current scenario. The proposed technique has provided a strong COVID-19 paediatric cavity telecare system. Thus, it will defend the Man-In-The-Middle attacks inside the noisy channel in this excessive use of digital transaction in the COVID-19 era.

Telecare paediatric dentistry is an approach to embed information and communication technology with dental health [10]. Dasgupta and Deb [11] have told that telecare is a new direction in the health care system. Chen *et al*. [12] had given a dimension of telemedicine on dental medicine care in 2003. Flanders [13] had shown the effectiveness of dental education schemes in schools in the year 1987. Distance is one of the obstacles behind improper paediatric treatments in dental fields. Cook *et al.* [3] and Morosini [14] expert online orthodontic opinions from remote dentists were taken for better treatment facilities.

But the biggest threat in such a TIS is the security issues. Intruders will grasp the medical data and signals, and they would proceed in illegal ways, maybe in terms of fake media claims, publicity, and assault, Bhowmik *et al.* [15] have proposed a computational intelligence and lossless regeneration on intraoral image transmission in 2019. Sarkar *et al.* [16] had proposed an efficient and secured sharing of gingivitis in 2018. Dey *et al.* [17] have proposed a metaheuristic approach towards the secured transmission of electronic prescriptions on the dental domain in 2019.

Hamming in the year 1950 [18] had introduced the idea of error detection and correction on the transmitting data. It is a linear block wise error detection and error correction on binary bits. Saiz-Adalid *et al.* [19] had modified Hamming codes by extending a parity bit to enhance its performances. Ullah *et al.* had shown a convenient way for detection of errors using Hamming codes [20]. Ahmadpour *et al.* [21] have proposed a new formulation technique on Hamming codes.

Bryk *et al.* [22] had designed encryption techniques using reversible logic gates in the year 2016. Picton [23] had developed modified Fredkin gates in logic design circuits in 1994. Datta *et al.* [24] had proposed reversible logical applications in the field of cryptography and coding theory in 2013. Bapannadora *et al.* [25] have designed an AES algorithm using a reconfigurable reversible logic circuit.

The inspiration driving fostering this novel NCK based encryption is to improve the distant clinical help to the paediatrics in this basic coronavirus times. Paediatrics are the most vulnerable in terms of coronavirus. They should be protected from such deadly virus. Because of lockdown limitations, the majority of the non-critical children are prescribed to be done in virtual consultations from isolates. This curtails the COVID-19 transmission to the children. It gives huge inspiration to proposed plans such COVID-19 Pediatric cavity telecare system.

Any health-related issues towards their child are the most important and stressed factor contributing to parents' anxiety. In this era of the global pandemic, parents' anxiety has raised exponentially towards their children. They are more concerned towards their child's health. Such a disease like paediatric cavities needs to be treated carefully without disclosing the facts to the eavesdroppers. The advantage of this paper is to provide a security layer on a child's dental image, so that intruders can do nothing with those encrypted partial shares if retrieved. The existing intraoral secret image sharing technique has some demerits, which are a few listed: i) Key exchange in TIS between the terminals in this COVID-19; ii) Secret sharing of intraoral images are ready available for distribution to illegal concerned persons keeping the parents in complete blind state of information; iii) Secret intraoral partial images are forwarded in a single link. The secret image will not be regenerated if the link is abrupt; iv) Distorted image, if transmitted, then secured transmission prompts to wrong treatment actions.

Dental cavities are frequent and common periodontal disease which affects the periodontium of children in rural areas of India. It has been seen in this pandemic era too. Cavities are caused by the bacteria infection inside the mouth to form the plaques, which then enamel eroding acids are generated to form the cavity in the teeth. A prominent and potential infrastructure in the field of palliative care is lagging in every sphere. A palliative care support system provides expert disease diagnosis along with proper treatment to cure the children. In addition, it provides huge mental support and care to such affected children. Availability of expertise persons such as paediatric dentists, general physicians, anaesthetics, paediatricians, and dieticians are not always found. Moreover, an acute crisis of clinical support systems like digital X-Ray clinics, and pathological laboratories are observed firmly. Such bare essential needs are more lacking more due to contemporary lockdown and social distancing constraints. Such supports are the minimum requirements to conduct a dental care system in proper fashion. Rural children having cavities in their single or multiple teeth suffer a lot to get better treatment.

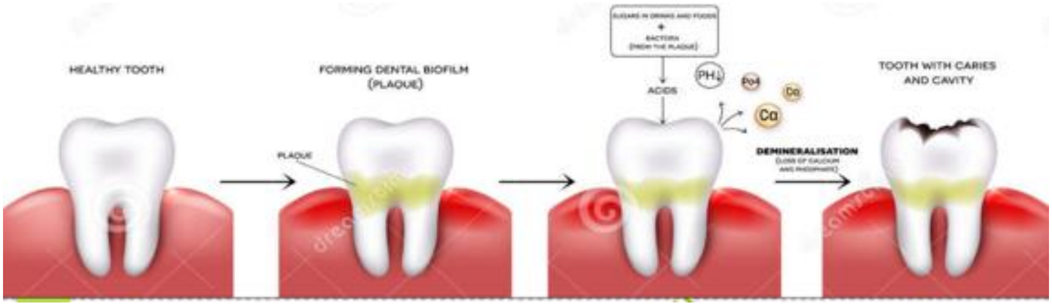
HEALTHY TOOTH
FORMING DENTAL BIOFILM (PLAQUE)
PLAQUE
SUGARS IN DRINKS AND FOODS + BACTERIA (FROM THE PLAQUE)
ACIDS
PH↓
Po4
Ca
Ca
DEMINERALISATION
(LOSS OF CALCIUM AND PHOSPHATE)
TOOTH WITH CARIES AND CAVITY

Figure 2. Transition of healthy paediatric teeth to formation of cavity

Unfortunately, children suffering from painful cavities do not get proper expert opinions due to social and infrastructural deficits. Thus, their disease remains untreated and conditions lead to extraction of teeth. In most of the remote villages paediatric dentists are almost not found as a regular practitioners.

The demerits discussed in the above section are solved using the proposed technique. Paediatric cavity image is secretly converted into reversible Fredkin structures [24], [25]. A parity based on Hamming codes key will be generated by the sender of TIS. The key will be diffused with the converted so called reversible image. The encrypted image is fed into Rivest-Shamir-Adleman (RSA) with the public key of the corresponding dentists of TIS.

In this proposed model of work, the above stated problem with respect to the dental domain can be solved. Children's medical data is more confidential enough. A secured paediatric image is to be transmitted over TIS for expert opinion. This would diagnose the child's disease better. Thus, keeping the children safe from the coronavirus attacks, their treatments are possible securedly through this proposed technique.

2. RESEARCH METHOD

The block diagram of Fredkin gate [26], [27] is given in Figure 3. It has three inputs and three outputs. The function of this reversible gate is given at (1), which has been adopted by the sender and receiver of TIS.

$$f(A,B,C) \rightarrow \{A, A'B + AC, AB + A'C\} \qquad (1)$$

A
B
C
Fredkin Gate
X
Y
Z

Figure 3. Block diagram of Fredkin gate

In this proposed technique, the intraoral paediatric image has been converted into binary matrix using Fredkin gate. An NCK of desirable length is obtained through the proposed Hamming code based parity scheme. Successive diffusion operations were performed on the said two resultants. Finally, the encrypted binary image will be transmitted to TIS by RSA using the public key of the dentist.

2.1. Proposed algorithm: NCK encryption

```
Input(s): Intraoral image (P1.JPEG[Total_Row ][Total_Col ] ),
Dentist's Public Key(DK[ ])
Output(s): Encrypted Intraoral Image
 {/* Paediatric Image to Binary Matrix Convert */}
For i = 0 to Total_Row
 For j = 0 to Total_Col
 Bin_Img[i][j] = Call BinaryImage( P1.JPEG[][])
 End for
End for
{/* Binary Image to Fredkin Image */}
For i = 0 to Total_Row
For j = 0 to Total_Col
 F_Img[i][j] = Call FredkinConvert( Bin_Img[Total_Row][Total_Col])
 End for
End for
{/* Chain Key Generation */}
KEY[ ] ← Call ChainKeyGen( PRNG S[ ])
{/* Encryption of P1.JPEG with KEY [ ] */}
For i = 0 to Total_Row
For j = 0 to Total_Col
 ENCRYPTED_IMAGE[i][j] = XOR(F_Img[i][j], KEY[ ])
 Increment j;
 End for
Increment i
 End for
 {/* RSA Encryption of Encrypted Image with Dentist's Public key */}
 Transmitted[ ][ ] = Call RSA (ENCRYPTED_IMAGE[Total_Row][Total_Col], DK[ ] )
```

2.1.1. Proposed algorithm: chain key generation

```
Input(s): No.of Parity Bits(PR), Length of Chain Key (KEYLEN), No.Of Sub Blocks (BlockLen)
Output(s): Chain Key Generation (HKEY [KEYLEN])
For i = 0 to BlockLen
 R0[i] = RND( ) MOD 2
End for
Assign K0 [Len] ≤ ( $2^{PR}$+ 1 )
K[0] ← Call HammingParityBitFill( R[0] )
For i = 0 to ( KEYLEN / BlockLen)
        $KEY_{PREV}$← Call Converted($KEY_{PREV}$)
 C ← CountNoOf1s ($KEY_{PREV}$)
        IF (Call ParityCheck ($KEY_{PREV}$)) THEN
         $KEY_{NEXT}$ ← {$KEY_{PREV}$ − $2^C$} XOR RO[BlockLen]
        Else
         $KEY_{NEXT}$ ← {$KEY_{PREV}$ + $2^C$} XOR RO[BlockLen]
        End if
 Increment i
 C ← 0
 HKEY [KEYLEN] ← $KEY_{PREV}$ CONCATENATION $KEY_{NEXT}$
End for
Return HKEY[KEYLEN]
```

2.1.2. Proposed algorithm: key conversion

```
Input(s): $Keystream, KS[Size]$
Output(s): $Converted\ Keystream, CKS[Size]$
$For\ i = 0\ to\ (Size - 1)$
$If\ (\ i = 0\ )\ Then$
        $CKS[i] = KS[i]$
 Else
$CKS[i] = KS[i]\ XOR\ KS[i-1]$
 $End\ if$
$Increment\ i$
$End\ for$
$Return\ (CKS[Size])$
```

3. RESULTS SECTION

In this section, results were briefly discussed. The above stated proposed algorithm was carried out on the high level language with modern computer configurations. Table 1 contains the exemplary data set of observation. Intermediate keys are well tabulated Table 1 for length of seed value, length of intermediate key, and desired key size are 4 bits, 7bits, and 70 bits respectively.

Table 1. Intermediate key formation with their decimal equivalences

Intermediate key (IK1)	Decimal (IK1)	Intermediate key (IK2)	Decimal (IK2)	Intermediate key (IK3)	Decimal (IK3)	Intermediate key (IK4)	Decimal (IK4)
0011001	25	0110011	51	1011010	90	1001100	76
0010100	20	0001001	09	1101101	109	0010110	22
0110111	55	0101110	46	0100001	33	1000001	65
0111101	61	0001110	14	1100011	99	0110101	53
0111010	58	0110100	52	0000000	00	0110011	51
0001110	13	0101101	45	1011001	89	1101110	110
1100100	100	1001000	72	0001111	15	0000101	05
1010111	87	1101111	111	1010000	80	1000011	67
1100101	101	1100011	99	0110010	50	0100110	38
1101110	109	1101101	109	1000001	65	1101001	105

Four intermediate keys were taken into considerations: IK1, IK2, IK3, and IK4.the first key, IK1 is the initial set of keys. The robustness of the proposed technique may be explained in terms that by changing single/double/triple bits of the seed value, we get drastic changes in their corresponding decimal values. Such changes are quiet random in nature and do not have any matching patterns. The centroid mean over their corresponding decimal are 62.9, 60.8, 63.0 and 59.2 respectively. Hence the intruders will be in big doubt to detect the exact key composition.

3.1. Graphical analysis

Figures 5-16 contain the graphs for histogram, floating frequency, and autocorrelation using the proposed keys, IK1, IK2, IK3, and IK4 respectively after proposed encryption. Histograms graphs are evenly poised as observed in those figures. Floating frequency graphs are uniformly spread throughout the character set. No similar patterns were found in the graphs of the autocorrelation. During the hyper digitization of telehealth, intruders cannot guess/assume any pattern from the cipher text of our technique. This could be a blossom for paediatric telehealth system in the COVID-19 pandemic time. Thus, it may be well said that intruders cannot guess the exact key composition to grasp the paediatric cavity intraoral images. Thus, the confidentiality of any children will be maintained in these proposed COVID-19 telecare information system.

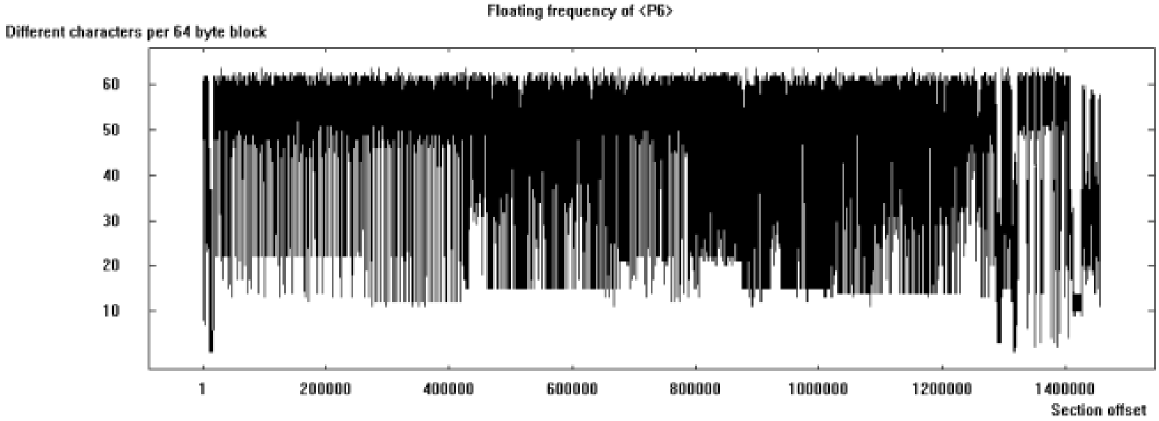

Figure 5. Histogram of Paediatric Cavity with NCK_ID =IK1

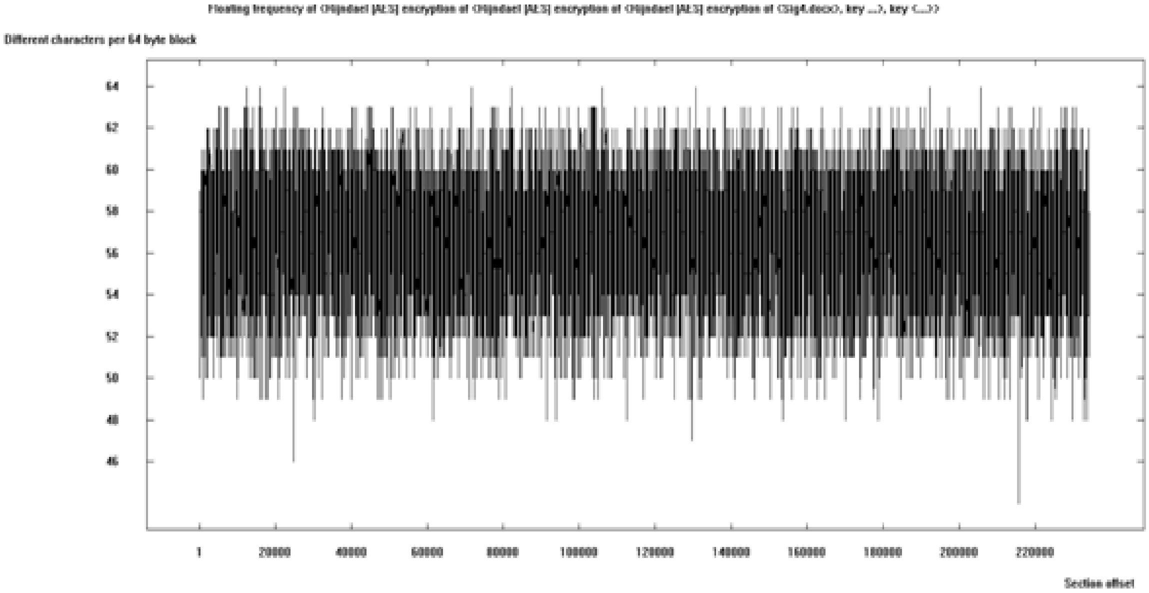

Figure 6. Floating Frequency of Paediatric Cavity with NCK_ID =IK1

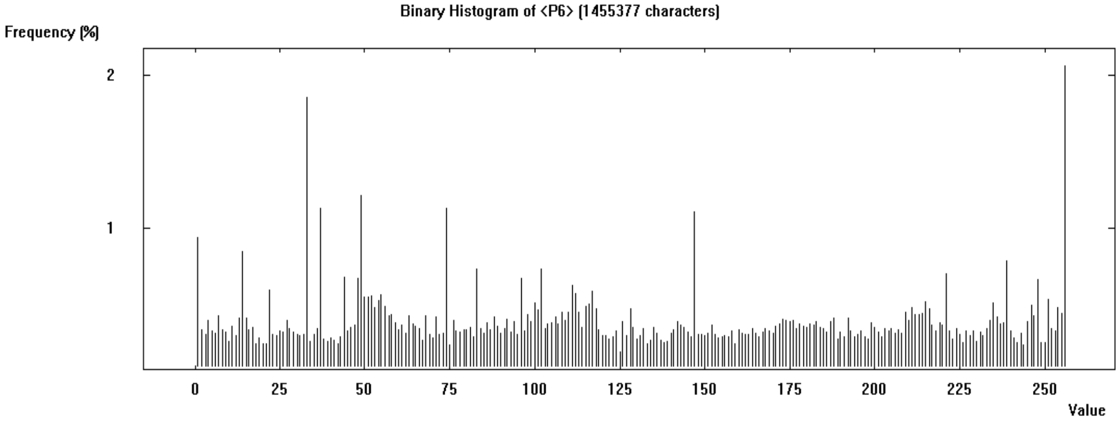

Figure 7. Autocorrelation of paediatric cavity with NCK_ID =IK1

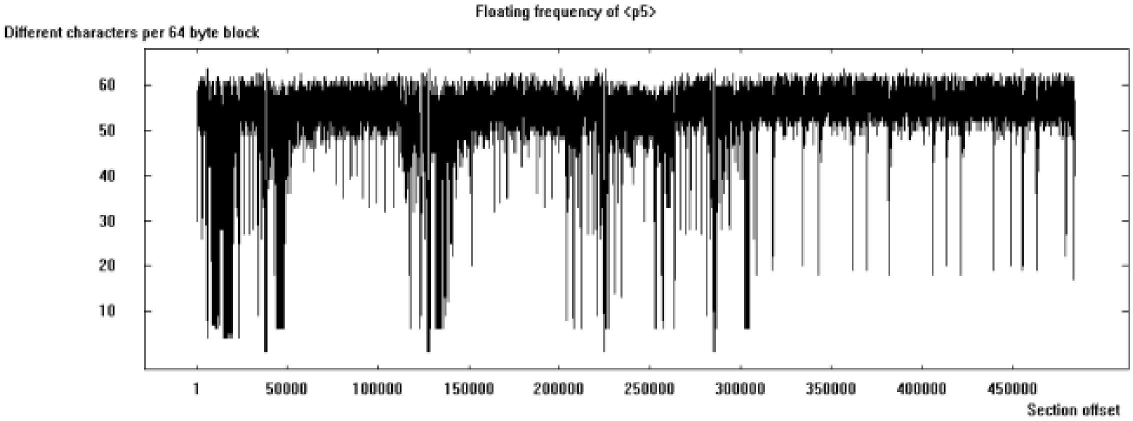

Figure 8. Histogram of paediatric cavity with NCK_ID =IK2

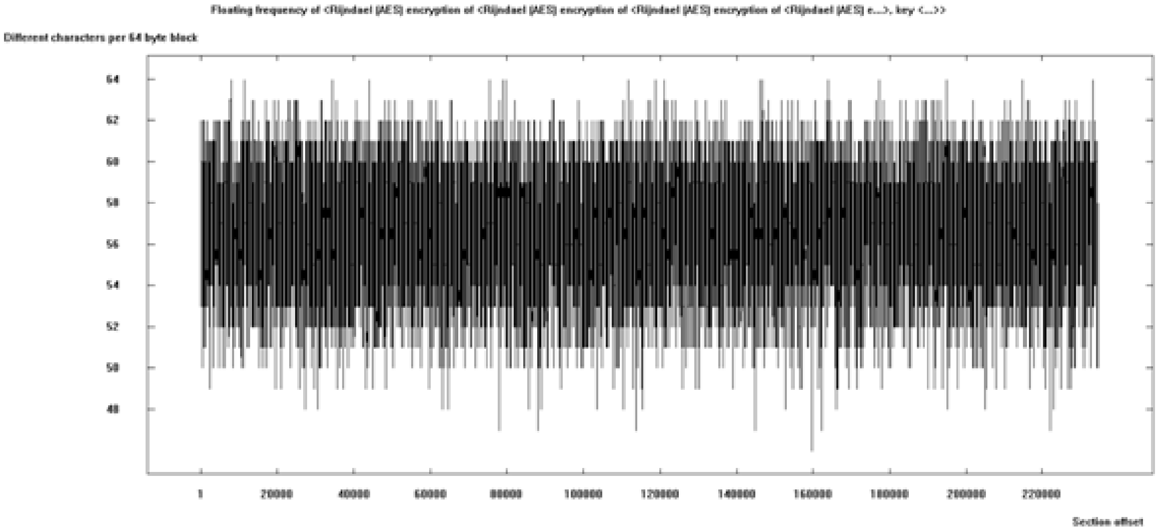

Figure 9. Floating frequency of paediatric cavity with NCK_ID =IK2

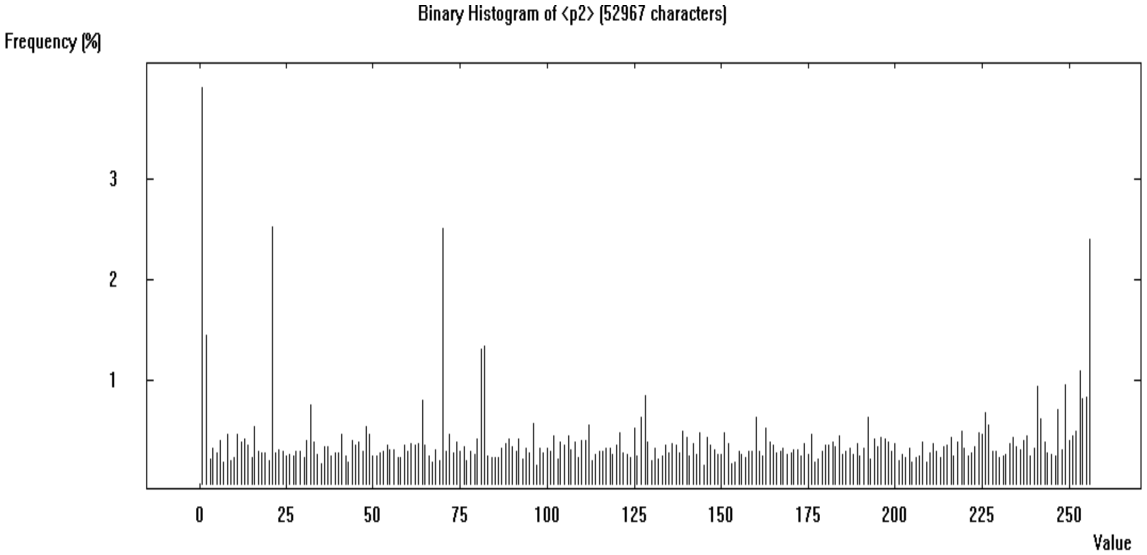

Figure 10. Autocorrelation of paediatric cavity with NCK_ID =IK2

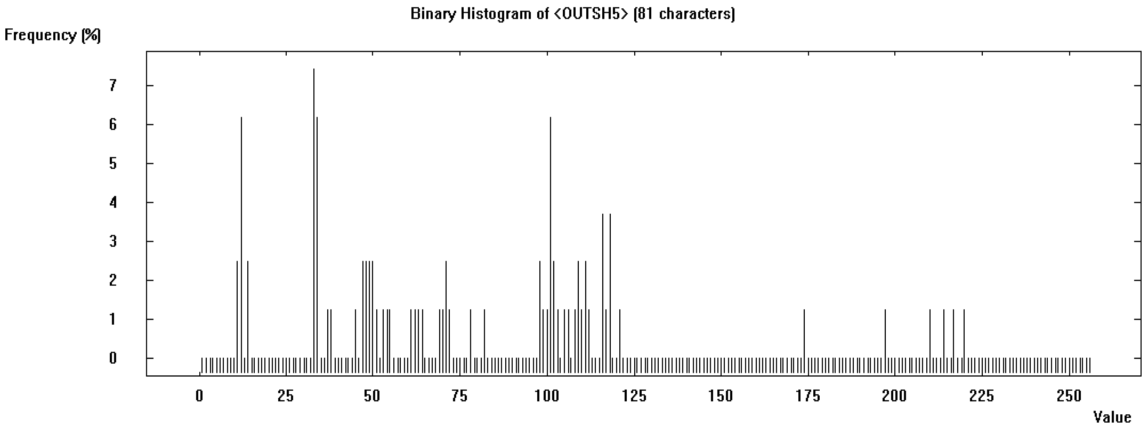

Figure 11. Histogram of paediatric cavity with NCK_ID =IK3

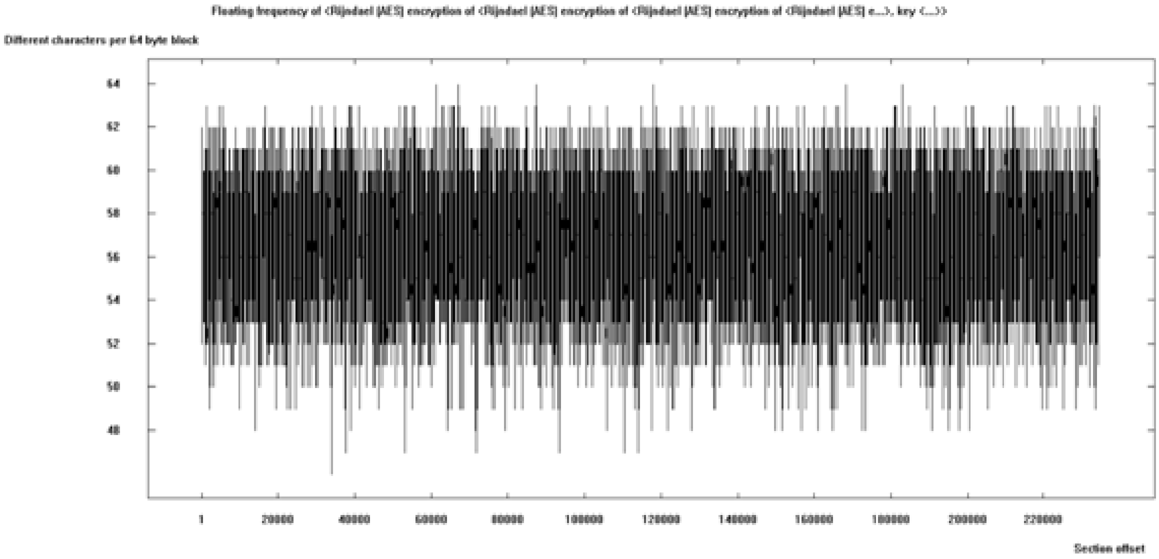

Figure 12. Floating frequency of paediatric cavity with NCK_ID =IK3

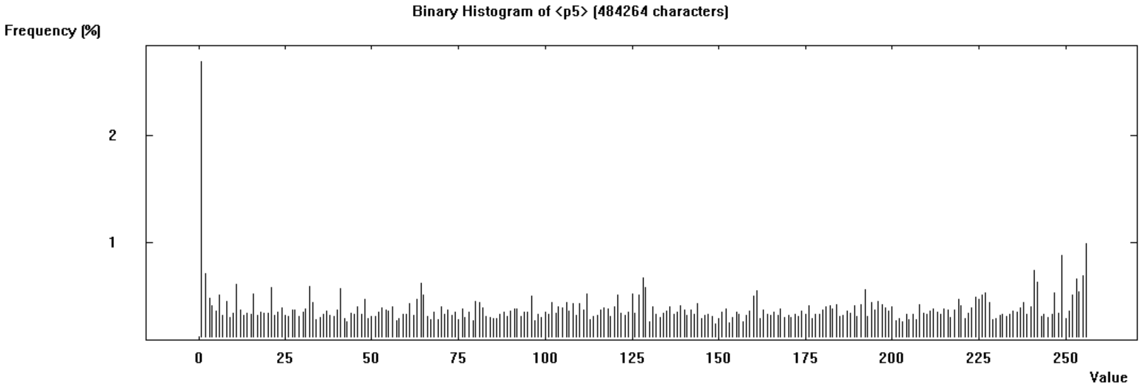

Figure 13. Autocorrelation of paediatric cavity with NCK_ID =IK3

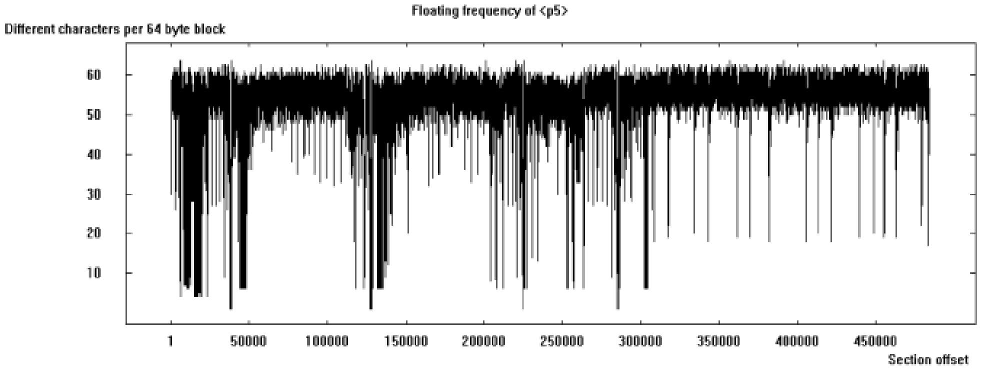

Figure 14. Histogram of Paediatric Cavity with NCK_ID =IK4

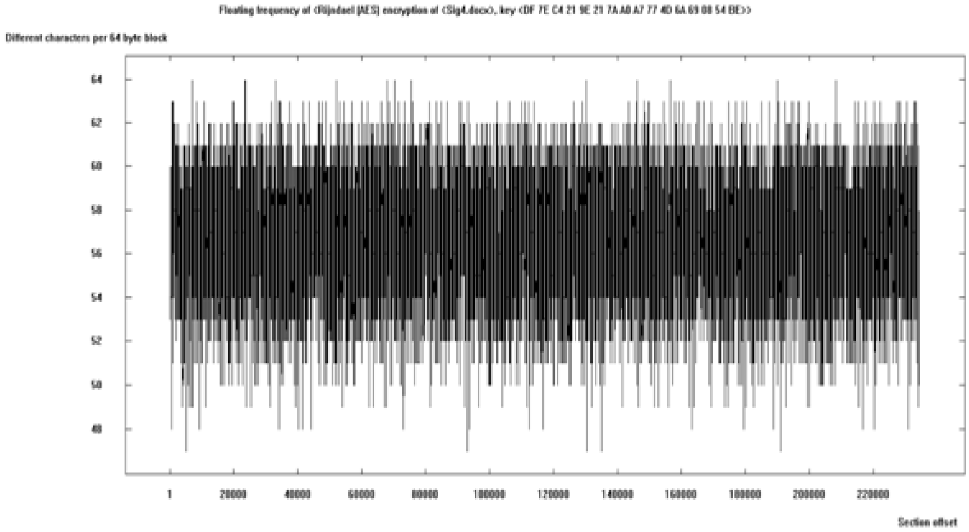

Figure 15. Floating Frequency of Paediatric Cavity with NCK_ID =IK4

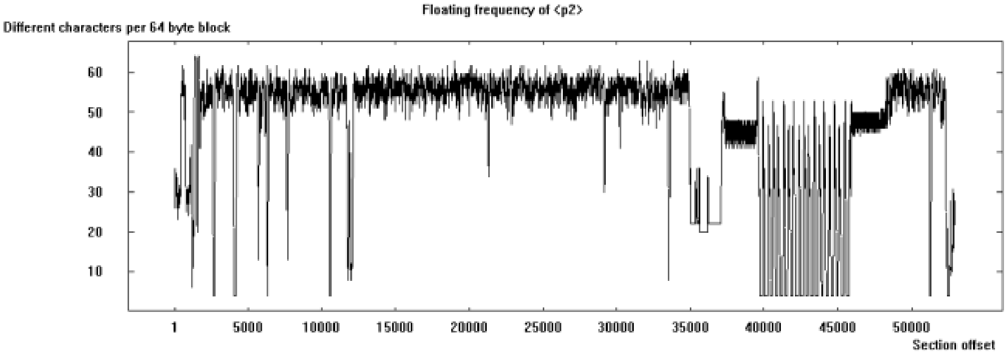

Figure 16. Autocorrelation of paediatric cavity with NCK_ID =IK4

3.2. Session key generation time comparison

The session key is the most vital issue in any cryptographic scheme [28]–[30]. In this sub-segment, we have compared the session key generation time needed. The proposed NCK generation on paediatric COVID-19 has been compared with some of the classical algorithms of cryptographic engineering. Table 2 has shown the needful timing comparisons. The proposed NCK technique has an acceptable time value for its key generation, when compared with others. This proves the efficacy of the proposed system.

Table 2. Time needed for key generation

Sl. No.	Technique	Key generation time (ms)
1	Proposed here	514.61
2	IDEA	492.47
3	RC5	615.21
4	RC6	511.25

3.3. Computing time comparison

The acceptance of any online TIS depends on the amount of time needed for its secured communication between the patient and the physicians. In Table 3, the encryption and decryption time were evaluated in seconds. It has been observed that the proposed technique operates successfully on different categories of paediatric cavity images in fewer time frames. Thus, it raised its acceptance factor in society [31]. The proposed NCK technique has a better computing time value as compared with the existing cryptographic methods. This proves the efficacy of the proposed NCK based cryptography.

Table 3. Proposed encryption – decryption time comparison with existing techniques

Sl. No.	Time observed (ms)	Proposed here	IDEA	RC5	RC6
1	Encryption	1.9875	1.7240	2.0148	1.9654
2	Decryption	1.6108	1.5507	1.7581	1.7058
3	Total time	3.5983	3.2747	3.7729	3.6712

3.4. Key size comparison

In this sub-section, a key length comparative study was done on the proposed NCK with other methods. Table 4 contains such values.

Table 4. Session key length comparison

Sl. No.	Technique	Key size (bits)
1	Proposed here	70
2	IDEA	128
3	RC5	128
4	RC6	128, 192, or 256

3.5. Comparison with earlier works

We have compared our proposed NCK method with some of the earlier papers on similar domain. Table 5 has been filled to draw the needed comparisons.

Table 5. Comparison with other papers

Sl. No.	Comparison conditions	[32]	[33]	[34]	[35]	[36]	Proposed here
1	Paediatric telehealth	No	No	Yes	No	Yes	Yes
2	Telepsychiatry	No	No	No	No	No	Yes
3	Child’s live data sensing	No	No	No	No	No	No
4	Session key generation	Yes	Yes	Yes	Yes	Yes	Yes
5	Data encryption	Yes	Yes	Yes	Yes	Yes	Yes
6	Data compression of children	No	No	Yes	No	No	No
7	Analysis on session key space	No	No	No	No	Yes	No
8	Histogram graph	No	No	No	No	Yes	Yes
9	Floating character frequency	No	No	No	No	Yes	Yes
10	Autocorrelation graph	Yes	No	No	No	Yes	Yes
11	Key generation time	No	Yes	No	No	Yes	Yes
12	Computing time calculation	No	No	No	No	Yes	Yes
13	Intermediate key values	No	No	No	No	No	Yes
14	Comparison	No	No	No	No	Yes	Yes

4. CONCLUSION

The proposed technique is an inevitable gesture towards an online COVID-19 telecare information system in terms of secured medical data transmission. Precautionary measures must be taken amidst COVID-19. In this unprecedented pandemic, telemedicine has become a substitute way of treating children. Security mechanisms must be ensured in telemedicine. They are at high risk of outside exposure to coronavirus. The results which were discussed in the earlier section show the robustness of the proposed technique. By flipping a single bit/multiple bits of the seed value, the key structure changes rapidly. This change has strongly been influential in compliance with histogram, floating frequency, and autocorrelation. The time for proposed key generation has been found to be 514.61 ms. The total cryptographic time has been noted as 3.5983 ms in this technique. Thus, making the intruders' role to be more critical, as every session has developed a changed seed value. In the era of such advanced technological domain, such paediatric COVID-19 telecare information systems would be highly rated and appreciated.

The concept of dynamic key length of NCK in this proposed technique may be added in future plan. Thus, different key lengths will be used for different paediatric medical communications. The intruders will have no knowledge on the size of the key length. It would highly strengthen the security policies of the proposed NCK.

ACKNOWLEDGEMENTS

The author deeply shows his gratitude to Dr Sunil Karforma, Head & Professor, Department of Computer Science, The University of Burdwan.

REFERENCES

[1] E. M. Strehle and N. Shabde, "One hundred years of telemedicine: does this new technology have a place in paediatrics?," *Archives of Disease in Childhood*, vol. 91, no. 12, pp. 956–959, Jul. 2006, doi: 10.1136/adc.2006.099622.

[2] D. T. Golder and K. A. Brennan, "Practicing dentistry in the age of telemedicine," *Journal of the American Dental Association*, vol. 131, no. 6, pp. 734–744, Jun. 2000, doi: 10.14219/jada.archive.2000.0272.

[3] J. Cook, J. Edwards, C. Mullings, and C. Stephens, "Dentists' opinions of an online orthodontic advice service," *Journal of Telemedicine and Telecare*, vol. 7, no. 6, pp. 334–337, Dec. 2001, doi: 10.1258/1357633011936967.

[4] W. Stallings, *Cryptography and network security: principles and practice*, 3rd ed. Pearson, 2004.

[5] N. Koblitz, "A course in number theory and cryptography," vol. 114, 1994, doi: 10.1007/978-1-4419-8592-7.

[6] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978, doi: 10.1145/359340.359342.

[7] J. Dey, A. Bhowmik, A. Sarkar, and S. Karforma, "Privileged authenticity in reconstruction of digital encrypted shares," *IAES International Journal of Artificial Intelligence*, vol. 8, no. 2, pp. 175–180, Jun. 2019, doi: 10.11591/ijai.v8.i2.pp175-180.

[8] A. Sarkar, J. Dey, A. Bhowmik, J. K. Mandal, and S. Karforma, "Computational intelligence based neural session key generation on E-health system for ischemic heart disease information sharing," in *Advances in Intelligent Systems and Computing*, vol. 812, 2019, pp. 23–30.

[9] A. Bhowmik, A. Sarkar, S. Karforma, and J. Dey, "A symmetric key based secret data sharing scheme," in *International Journal of Computer Sciences and Engineering*, 2019, vol. 7, no. 1, pp. 188–192.

[10] J. M. Birnbach, "The future of teledentistry," *Journal of the California Dental Association*, vol. 28, no. 2, pp. 141–143, Feb. 2000.

[11] A. Dasgupta and S. Deb, "Telemedicine: A new horizon in public health in India," *Indian Journal of Community Medicine*, vol. 33, no. 1, p. 3, 2008, doi: 10.4103/0970-0218.39234.

[12] J. W. Chen, M. H. Hob-Dell, K. Dunn, K. A. Johnson, and J. Zhang, "Teledentistry and its use in dental education," *Journal of the American Dental Association*, vol. 134, no. 3, pp. 342–346, Mar. 2003, doi: 10.14219/jada.archive.2003.0164.

[13] R. A. Flanders, "Effectiveness of dental health educational programs in schools," *The Journal of the American Dental Association*, vol. 114, no. 2, pp. 239–242, Feb. 1987, doi: 10.14219/jada.archive.1987.0033.

[14] I. de A. C. Morosini, D. C. De Oliveira, F. de M. Ferreira, F. C. Fraiz, and C. C. Torres-Pereira, "Performance of distant diagnosis of dental caries by teledentistry in juvenile offenders," *Telemedicine and e-Health*, vol. 20, no. 6, pp. 584–589, Jun. 2014, doi: 10.1089/tmj.2013.0202.

[15] A. Bhowmik, J. Dey, A. Sarkar, and S. Karforma, "Computational intelligence based lossless regeneration (CILR) of blocked gingivitis intraoral image transportation," *IAES International Journal of Artificial Intelligence*, vol. 8, no. 3, pp. 197–204, Dec. 2019, doi: 10.11591/ijai.v8.i3.pp197-204.

[16] A. Sarkar, J. Dey, A. Bhowmik, J. K. Mandal, and S. Karforma, "Energy efficient secured sharing of intraoral gingival information in digital way (EESS-IGI)," in *Communications in Computer and Information Science*, 2018, vol. 836, pp. 584–599, doi: 10.1007/978-981-13-1343-1_49.

[17] J. Dey, S. Karforma, A. Sarkar, and A. Bhowmik, "Metaheuristic guided secured transmission of E-prescription of Dental disease," *International Journal of Computer Sciences and Engineering*, vol. 7, no. 1, pp. 179–183, 2019.

[18] R. W. Hamming, "Error detecting and error correcting codes," *Bell System Technical Journal*, vol. 29, no. 2, pp. 147–160, Apr. 1950, doi: 10.1002/j.1538-7305.1950.tb00463.x.

[19] L. J. Saiz-Adalid, P. Gil, J. C. Baraza-Calvo, J. C. Ruiz, D. Gil-Tomas, and J. Gracia-Moran, "Modified hamming codes to enhance short burst error detection in semiconductor memories," in *Proceedings - 2014 10th European Dependable Computing Conference, EDCC 2014*, May 2014, pp. 62–65, doi: 10.1109/EDCC.2014.25.

[20] R. Ullah, J. Khan, S. Latif, and I. Ullah, "Convenient way for detecting check bits in hamming code," in *Communications in Computer and Information Science*, 2011, vol. 256 CCIS, pp. 344–356, doi: 10.1007/978-3-642-26010-0_42.

[21] A. Ahmadpour, A. Ahadpour Sha, and M. Ziabari, "A novel formulation of Hamming Code," in *2009 6th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology*, May 2009, pp. 808–811, doi: 10.1109/ecticon.2009.5137169.

[22] M. Bryk, K. Gracki, P. Kerntopf, M. Pawlowski, and A. Skorupski, "Encryption using reconfigurable reversible logic gate and its simulation in FPGAs," in *2016 MIXDES - 23rd International Conference Mixed Design of Integrated Circuits and Systems*, Jun. 2016, pp. 203–206, doi: 10.1109/MIXDES.2016.7529732.

[23] P. D. Picton, "Modified Fredkin gates in logic design," *Microelectronics Journal*, vol. 25, no. 6, pp. 437–441, Sep. 1994, doi: 10.1016/0026-2692(94)90068-X.

[24] K. Datta and I. Sengupta, "Embedded tutorial: Applications of reversible logic in cryptography and coding theory," in *2013 26th International Conference on VLSI Design and 2013 12th International Conference on Embedded Systems*, Jan. 2013, pp. lxvi--lxvii, doi: 10.1109/VLSID.2013.146.

[25] R. Bapannadora, P. Ashok, and K. Tirupathaiah, "An advanced encryption standard using reconfigurable reversible logic gates," *International Journal For Innovative Research In Multidisciplinary Field*, vol. 3, no. 3, pp. 113–118, 2017.

[26] E. Fredkin and T. Toffoli, "Conservative logic," *International Journal of Theoretical Physics*, vol. 21, no. 3–4, pp. 219–253, Apr. 1982, doi: 10.1007/BF01857727.

[27] A. Banerjee, "Reversible cryptographic hardware with optimized quantum cost and delay," in *2010 Annual IEEE India Conference (INDICON)*, Dec. 2010, pp. 1–4, doi: 10.1109/INDCON.2010.5712605.

[28] H. N. Khan, A. Chaudhuri, A. Das, and A. Chaudhuri, "An ultra robust session key based image cryptography," *Microsystem Technologies*, vol. 26, no. 7, pp. 2193–2201, Jul. 2020, doi: 10.1007/s00542-019-04518-9.

[29] L. A. Tharakan, S. Daniel, and R. Dhanasekaran, "Security enhancement and monitoring for data sensing networks using a novel asymmetric mirror-key data encryption method," in *AI and Machine Learning Paradigms for Health Monitoring System*, 2021, pp. 65–78.

[30] O. Reyad and M. E. Karar, "Secure CT-image encryption for COVID-19 infections using HBBS-based multiple key-streams," *Arabian Journal for Science and Engineering*, vol. 46, no. 4, pp. 3581–3593, Apr. 2021, doi: 10.1007/s13369-020-05196-w.

[31] J. Dey, A. Sarkar, and S. Karforma, "Newer post-COVID perspective: Teledental encryption by de-multiplexed perceptrons," *International Journal of Information Technology*, vol. 13, no. 2, pp. 593–601, Apr. 2021, doi: 10.1007/s41870-020-00562-1.

[32] M. Ahmad, O. Farooq, S. Datta, S. S. Sohail, A. L. Vyas, and D. Mulvaney, "Chaos-based encryption of biomedical EEG signals using random quantization technique," in *2011 4th International Conference on Biomedical Engineering and Informatics (BMEI)*, Oct. 2011, pp. 1471–1475, doi: 10.1109/BMEI.2011.6098594.

[33] C.-F. Lin, S.-H. Shih, and J.-D. Zhu, "Chaos based encryption system for encrypting electroencephalogram signals," *Journal of Medical Systems*, vol. 38, no. 5, p. 49, May 2014, doi: 10.1007/s10916-014-0049-6.

[34] M. Raeiatibanadkooki, S. R. Quchani, M. M. KhalilZade, and K. Bahaadinbeigy, "Compression and encryption of ECG Signal using wavelet and chaotically Huffman code in telemedicine application," *Journal of Medical Systems*, vol. 40, no. 3, pp. 1–8, Mar. 2016, doi: 10.1007/s10916-016-0433-5.

[35] C. F. Lin, "Chaotic visual cryptosystem using empirical mode decomposition algorithm for clinical EEG signals," *Journal of Medical Systems*, vol. 40, no. 3, pp. 1–10, Mar. 2016, doi: 10.1007/s10916-015-0414-0.

[36] M. A. Murillo-Escobar, L. Cardoza-Avendaño, R. M. López-Gutiérrez, and C. Cruz-Hernández, "A double chaotic layer encryption algorithm for clinical signals in telemedicine," *Journal of Medical Systems*, vol. 41, no. 4, p. 59, Apr. 2017, doi: 10.1007/s10916-017-0698-3.

BIOGRAPHIES OF AUTHORS

Joydeep Dey pursed Bachelor of Computer Application (Honours) from Cyber Research & Training Institute, Burdwan, India in 2007 and M.C.A. from the University of Burdwan in 2011 and he had secured First Class First (GOLD MEDALIST). He is working as State Aided College Teacher & Head in Department of Computer Science at M.U.C. Women's College, Burdwan since 2011. He has published 02 SCI indexed Springer journal paper , 06 SCOPUS Indexed journals, 02 Edited Book Chapters, 04 Book-Chapters (SPRINGER; SCOPUS INDEXED),03 International Conferences journals (UGC journals), and 35 others publications (International/National/State/Regional Level). His main research interest includes Cryptography and Computational Intelligence in Telehealth. He has more than 10 and 0.5 years of teaching experience at UG and PG level respectively. He can be contacted at email: joydeepmcabu@gmail.com.