Int. j. inf. tecnol. (April 2021) 13(2):593–601
https://doi.org/10.1007/s41870-020-00562-1

ORIGINAL RESEARCH

Newer post-COVID perspective: Teledental encryption by de-multiplexed perceptrons

Joydeep Dey[1] · Arindam Sarkar[2] · Sunil Karforma[3]

Received: 10 July 2020 / Accepted: 6 November 2020 / Published online: 2 January 2021

Abstract This paper presents an efficient mechanism for secured encryption of intraoral information in the emerging field of Teledental. Due to global rapid surge in the (Coronavirus Disease) COVID patients, the services of Teledental are best suited in the newer post-COVID era. A devised perceptron has been intelligently embedded with de-multiplexing ability to transmit data to the dentists has been proposed. Exact session key has been developed through learning rules applied on the perceptrons by both the patient and dentist. For simplicity, gingivitis data is highly recommended to transmit in a highly secured manner with patients' data integrity. Gingivitis is an important dental disease which is primarily caused by the bacterial colonization. It shows gum bleeding and inflammations in the gingiva. Encrypted transmission is required to the Dentist for early diagnosis and treatment in Teledental system in this pandemic context. Gingivitis data are then broken into parts by the demultiplexer followed by individual proposed header generation. It is predominantly done to confuse the intruders about the originality of the intraoral data. Chi-square, Avalanche, Strict Avalanche, etc. were carried on the proposed partial shares to generate good outcomes when compared to classical algorithms. To confuse the intruders, character frequency, floating frequency, and autocorrelation were tested extensively. It is a newer approach to avail the secured Teledental features in post-COVID time.

Keywords COVID · Gingivitis · Teledental · Perceptron · Demultiplexing

1 Introduction

Teledental systems are developed to serve the patients from distant locations in this post-COVID context. Patients are advised not to visit the dental clinics to avoid the corona virus attacks. More they stay at home, more they are safe from COVID attacks. Security parameter is the foremost criterion that needs to be addressed while transmitting information in Teledental systems. In classical cryptography [1–3], the information is accessed by the -intruders in context of sniphing, spoofing, phising, etc. Symmetric key cryptography [4] in Teledental system means the same key will be used by the patients and physicians for encryption and decryption respectively. Confidential data related to the patients need to be transmitted to the destination by using certain encryption technique. It is so done in order to resist the man in the middle attacks. Such encryption and decryption procedures are controlled by the concerned Teledental system. In medical sciences, data transmission using artificial neural architectures is an emerging area of research [5].

Tampering of dental data by the intruders lead to wrong diagnosis and failure in line of treatments. Unprotected data can easily be altered intentionally to leak out the

✉ Joydeep Dey
joydeepmcabu@gmail.com

Arindam Sarkar
arindam.vb@gmail.com

Sunil Karforma
sunilkarforma@yahoo.com

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

[2] Department of Computer Science and Electronics, R.K.M. Vidyamandira, Belur, WB, India

[3] Department of Computer Science, The University of Burdwan, Burdwan, WB, India

information. If the symmetric key used for encryption is somehow compromised by the attackers then the entire patients' data will be leaked to the unauthorized agents. The implementation of artificial neural networks (ANN) [6, 7] is a secure option for data transmission inside the Telecare E-Health system [8, 9]. A perceptron is a type of artificial neural network which has been considered in this proposed technique. It consists of input neurons, weights and a bias constant connected hidden neurons, and output neuron. The key idea is that two perceptrons are placed at the patient and dentist, and they do not exchange their keys between them. Learning rules are used to converge their weight vector into an identical session key. The intraoral information is broken into four parts; perceptron at the patient end is followed by a demultiplexer of size 1 × 4 (Fig. 1).

Proper oral care is always needed for everyone's healthy lifestyle. Gingivitis is a kind of periodontal disease. Its symptoms are gum swelling, bleeding, redness, soreness, etc. Deposition of bacterial plaque on the teeth surface is the initial symptom of such disease. Then the plaque is calcified to form tartar and thus causing the gingivitis. Gingivitis can be reversed in case of early detection provided the patient takes a constant and better oral hygiene. The best way to achieve it by a proper brushing technique and minimum twice daily [10–13]. In the advanced Telecare E-Health, the patients transmit her/his intraoral data to the specified dentist for diagnosis and treatment.

This paper presents an encryption technique based on perceptron that transmit the intraoral data by dismantling into sub-pieces of square matrix by devising through demultiplexer by the patient. Then encrypting with synchronized session key followed by header generation. The reverse end perceptron will decrypt the header portions from each share followed by decryption with synchronized session key one by one, then feeding into a multiplexer to reconstruct the original intraoral data. It deals with low computational cost and complexity incurred by the perceptron based neural network.

A secured encryption technique has been proposed to share the intraoral data by applying demultiplexing technique in the domain of Telecare E-Health. Aiming to make the intruders' task more difficult, a header generation has been proposed at each share. This paper has been organized in the following manner. Section 1 deals with the introductory part. Section 2 focuses some of the background and related tasks. Section 3 contains the problematic areas while transmitting data in Telecare systems. The novelty of the proposed technique has been illustrated in Sect. 4. Results and analysis are given in Sect. 5. Section 6 deals with the conclusion and those references are mentioned at the end.

2 Literature survey

2.1 Causes of gingivitis

Food habits and lifestyles are also responsible for gingivitis. The most common causes of gingivitis are poor oral hygiene which encourages the formation of plaque. Plaque is also formed when the starches and sugar in food interact with the oral bacterial microflora. Brushing and flossing each day removes plaque. Risk factors include certain viral and fungal infections, poor nutrition, older age, hormonal changes, etc. [14].

Gum diseases are being indicated by the early signs of gum bleeding. If treated early and on the right track, there is a possibility of reversing the conditions [15]. Gingivitis is certainly connected to diabetes and other related chronic diseases. A Fig. 2 depicts the image of gingivitis caused due to diabetes. In India, huge number of people suffers from diabetes, which leads to gingivitis in their lifespan [16, 17].

Other factors contributing largely to gingivitis are hormonal changes, stress and anxiety, malnutrition, some medications like phenytoin, amlodipine, cyclosporine, diabetes, immune compromization, dental caries, etc.

Fig. 1 Single layer feed forward perceptron

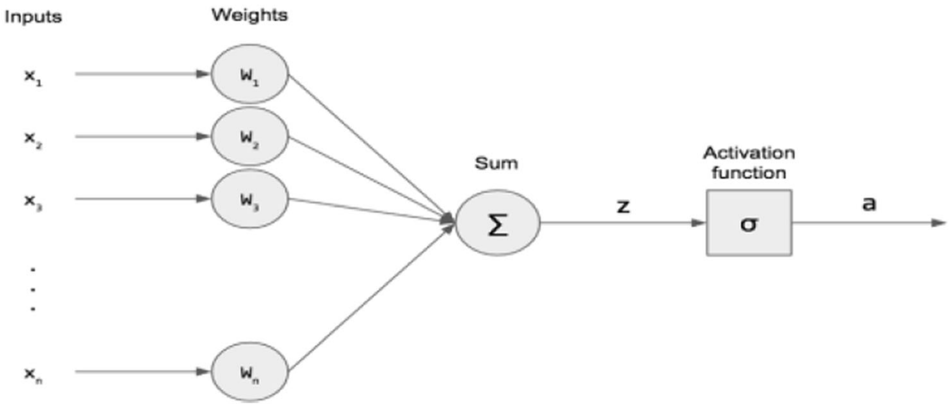

Fig. 2 Gingivitis caused due to diabetes

2.2 Use of perceptron in data transmission

In the field of Telcare E-Health, huge amount of extensive data are available for the research and transaction purposes [18–20]. So it is necessary to propose a model for the efficient data filtration and transmission. In the same regard, arrival of artificial neural networks has brought a higher degree of pace in medical data transmission [21–23]. An artificial neural network may be represented as a complex system [24] with higher dimensions, extensive interconnections, adaptability, and self-organizing features. Single layered and double layered feed forward neural networks were very useful in the recent decades in the domain of machine learning and big data analysis [23, 25]. A special type of feed forward neural network is the multilayer perceptron (MLP) [26, 27] having multiple hidden layers is more efficient to solve different types of nonlinear problems like pattern recognition, big data classification, numerical approximation, etc. Earlier research study had shown that single layer perceptrons outperform any continuous or discontinuous function with compared with multi layer perceptron [28]. Hence single layer perceptron are much better in data transmission domain. Mirjalili had shown that in the context of the back propagation neural networks, the starting values of the learning rate and the momentum factor lead to unsuitable divergence [29].

3 Problem specifications

The medical travelling throughout the Telecare network are the most vulnerable parts by the intruders. They are very much proactive to sense those patients' related confidential data, and then to forged them entirely. In Telecare E-Health systems, patient can take active participation from their home regarding their health issues. Similarly, dental issues can be addressed by such Telecare systems [5]. Despite of rapid developments in this sector, there are loopholes in those systems in the light of data security. An encryption algorithm is being considered as good as its keys are robust and sensitive. Moreover, the used encryption and decryption algorithms are open accessible by all agents. Only the key is kept secret between the patient and the dentist. Hence, by compromising the secret key, intruders are able to detect all confidential data. This is the area of concern in this proposed technique.

4 Proposed methodology

The key issue as stated in the earlier section has been addressed in this proposed paper. Structurally similar perceptrons are taken at the patient's and the dentist's Telecare system [8, 9]. The input set and the random weight vectors are same at both ends to achieve the synchronization. Based on the leaning rules of the perceptron, will adjust its weights till the best condition is not reached. Thus, in true sense, there will be no exchange of the secret key between the patient and dentist. Followed by the demultiplexing technique on the intraoral data, then a header generation has been proposed on all the partial shares [5]. The following algorithm will explain its technique in brief.

4.1 Algorithm: Proposed Perceptron based Key Generated Encryption

```
Input(s): Intraoral Data, G.JPEG, Input, Hidden, Output Perceptron Neurons as N, K, 1, one input to DEMUX,
Output(s): Four numbers of encrypted shares embedded with individual header.
$For\ i = 0\ to\ Pixel_{row}$ /* $Image\ to\ Binary\ Matrix\ Transformation$ */
  $For\ j = 0\ to\ Pixel\_column$
     $Bin\_Matrix[i][j] = ImageConvert2BinaryMatrix(G.JPG)$
$Epochs \leftarrow 0$
$While\ [Count\ != Max\_Epochs]$ /*Session Key Generation As Weight Vector by Perceptrons*/
        $X_i \leftarrow 1, X_1, X_2, \dots, X_N$ /* $Peceptron\ Input\ Vector\ Representation$ */
        $w[i] = PseudoRandomNumber(-1, +1)$ /* $Pseudo\ Random\ Weight\ Initialization$ */
              $Y \leftarrow w[B] + \sum_{i=1}^{N} w_i * X_i$ /* $Hidden\ Unit\ Output\ Generation$ */
$If\ (Y >= Net_{Target})\ Then$ /* $Output\ Unit\ Generation$ */
      $Z_i \leftarrow 1$
$Else$      $Z_i \leftarrow 0$
$If\ (Z_i\ != Net\_Target)\ Then$ /* $Learning\ Rule\ of\ Perceptron$ */
      $w_{Next} = w_{Prev} + \{LR * X_i\}$
      $B_{Next} = B_{Prev} + \{$ LR * Net_Target $\}$
$Else$
      $w_{Next} = w_{Prev}$ ,      $B_{Next} = B_{Prev}$
$Epochs \leftarrow Epochs + 1$
$For\ i = 1\ to\ 4$ /* $Demultiplexing\ Phase$ */
      $PartialShare[i][\,] = SplitShare(Bin\_Matrix[\,][\,])$
$m \leftarrow 1$ /*Encryption of data using Perceptron session key */
$For\ m = 1\ to\ 4\ do$
     $For\ i = 0\ to\ (Row / 2) - 1\ do$
       $For\ j = 0\ to\ (Col / 2) - 1\ do$
            $EncryptedShare[i][j] = PatialShare[i][j] \oplus WeightVector$
              $j = j + 1,\ m = m + 1$
         $i = i + 1$
$For\ i = 1\ to\ 4$ /* $Header\ Generation$ */
     $Call\ Header\ Generation(EncryptedShare, i)$
Four shares are being transmitted to the Dentist one by one.
```

4.1 Proposed header generation

Another novel part which has been proposed in this paper is to design a header structure for individual shares [5]. It consists of two attributes: quadrant number (QNo) and the total length of the partial share, which is dynamic in size. It depends on the length of the partial share generated by demultiplexer. The quadrant number is used for the reassembly by the dentist's perceptron. The following algorithm will illustrate the header generation.

```
Algorithm: Proposed Header Generation
Input(s): $Partial\ Share\ (PS), Iteration\ (It)$ Output(s): $Header\ Structure\ HS\ merged\ with\ Partial\ Share$
$QNo \leftarrow It$ /* $Header\ Generation$ */
 $TotLen \leftarrow SizeOf(PS)$
 $HS\,[3] = QNo\ ||\ TotLen\ ||\ PS$
```

5 Results analysis

An extensive analysis has been done on the proposed technique of encryption. The comparison study was carried out between the proposed technique and the existing RSA, 3-DES (168 bits), AES (128 bits) on thirty different types of files related to intraoral data. After compiling such files, a comparison which is emphasized on Avalanche test, Strict Avalanche tests and Bit Independence test has been carried out. Avalanche Test, Strict Avalanche Test and Bit Independence Test.

The study of comparison between the source intraoral file and proposed encrypted intraoral file to observe the magnitude of changes in its all bits has been done. Change in the encrypted bytes has been observed for every bit change with respect to the original intraoral byte in the entire sequence of communication in Telecare E-Health. Here, the standard deviation from the expected values were calculated and then subtract the ratio of the calculated standard deviation with expected value from 1.0 to get the

Table 1 Comparisons of average values on different files

Encryption method	Avalanche	Strict Avalanche	Bit independence
Proposed technique	0.9548012	0.9230287	0.4589960
RSA	0.9647844	0.9889471	0.5148289
3DES	0.9741924	0.9357021	0.5897012
AES	0.9012571	0.9597460	0.6004871

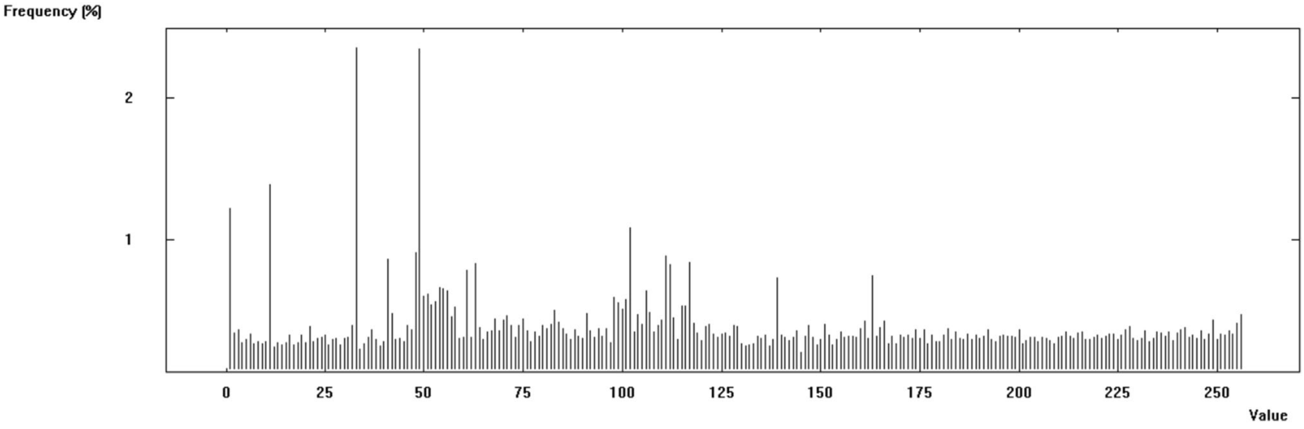

Fig. 3 Character frequency of plain intraoral file

Table 2 Comparisons of Chi-square average values

Source intraoral file (in bytes)	Proposed technique	3DES	AES
4,253,896	8,217,448	8,610,871	9,701,812
4,305,096	8,614,499	8,104,951	8,780,754
5,454,656	9,112,610	9,004,784	9,258,012
5,455,680	10,109,597	10,188,500	11,947,410
5,457,728	10,127,300	10,228,374	12,579,598

Avalanche and Strict Avalanche on a 0.0–1.0 scale. The Bit Independence test measures the correlation coefficient between the jth and kth components of the output difference string. If this correlation gets closer to 1.0 then it is said to have good Avalanche and Strict Avalanche criteria. In case of intraoral text files, there will be zero bytes between 128 and 255 bytes. The function of Bit Independence test can be written in the following Eq. 1:

$$f : \{0,1\}^n \{0,1\}^n, \tag{1}$$

for all i, j, k $\in \{0,1\}^n$,$j \neq k$, flipping input bit i will generate output bits j and k will change independently.

Thirty intraoral files of different sizes ranging from 3296 to $5,456,704$ bytes were considered for carrying out Avalanche test, Strict Avalanche test and Bit Independence test. The output of Avalanche test and Strict Avalanche test on those intraoral files encrypted using the proposed technique and existing techniques like RSA, 3DES, AES is almost equal to 1.0. The output of Bit Independence test is comparatively less than Avalanche test and Strict Avalanche test. Table 1 contains the observed data in this regard. In Fig. 3, a graphical representation has been put on the outputs listed in the above Table 1 for Avalanche test, Strict Avalanche test and Bit Independence test on their average data in the context of the proposed technique and existing techniques like RSA, 3DES and AES.

5.1 Non-homogeneity test

To find out the significant difference between the expected frequency and the actual frequency of the encrypted intraoral data, Pearson's Chi-square test has been used. Higher Chi-square value indicated better degree of encryption at the proposed technique. Thirty intraoral files of different sizes ranging from 3296 to 5,456,704 bytes were considered for performing Chi-square test. Table 2 represents Chi-square values obtained by the proposed technique, 3DES, and AES of thirty different intraoral files. The average Chi-square values obtained by the proposed technique, 3DES, and AES are 9,236,291, 9,227,496, and 10,453,517 respectively. There has been an increase in the Chi-square value when the intraoral file sizes increases. So,

Table 3 Comparative study w.r.t. existing algorithms

Sl. no.	Attributes	3DES	AES	Proposed technique
1	Size of blocks	64	128	128
2	Size of key	168	128/192/256	128
3	Key space size	2^{168}	$2^{128}/2^{192}/2^{256}$	2^{128}
4	Secret key exchange	Yes	Yes	No
5	Cipher type	Symmetric block	Symmetric block	Sequential symmetric block
6	Core algorithm used	Fiestel network	Substitution permutation network	Neural perceptrons
7	Data vulnerabilities	Brute force attacks	Side channel attacks	Considerably Secured
8	Processing speed	Very slow	Fast	Considerably fast

it may obtain better degree of security in proposed which is comparable with that of others.

5.2 Comparative tabulation with classical algorithms

In this section, a comparative study was conducted between the proposed technique and existing bench-mark classical 3DES and AES technique [30]. It has been observed that the proposed technique had yielded satisfactory results when compared with existing methods. The summary of this statement is given at Table 3.

5.3 Character frequencies, floating frequencies, autocorrelation analysis

In this section the analysis of character frequencies of thirty intraoral files were carried out examination by the proposed technique. The following Fig. 3 represents the spectrum which contains the frequency distribution of its characters for a single intraoral file. In the next Fig. 4, it contains the spectrum of its frequency distribution of the corresponding encrypted characters by the proposed method when applied on the same intraoral file. From these two figures, it can be stated that that the frequency distribution of characters are more widely distributed in the encrypted intraoral file [31]. The floating frequency analysis of thirty intraoral files was carried out here by the proposed technique. It is a characteristic of the local information content for the intraoral files at different points. The floating frequency indicates how many different characters of sixty four character long segment inside the source file. Figure 5 depicts the floating frequencies of its characters for a single intraoral file. The Fig. 6 indicates the spectrum of floating frequencies of the corresponding encrypted characters by using the proposed technique on the same intraoral file. By observing these two figures, it can be stated that floating frequencies of by the proposed technique shows higher degree of security. Analysis of autocorrelation of thirty different types of intraoral files was done by the proposed technique. Autocorrelation of a file is an index of the similarity at different points inside it. The spectrum of autocorrelation of characters when applied on the same intraoral file has been shown in the following Fig. 7. The spectrum of autocorrelation of encrypted file using the proposed technique can

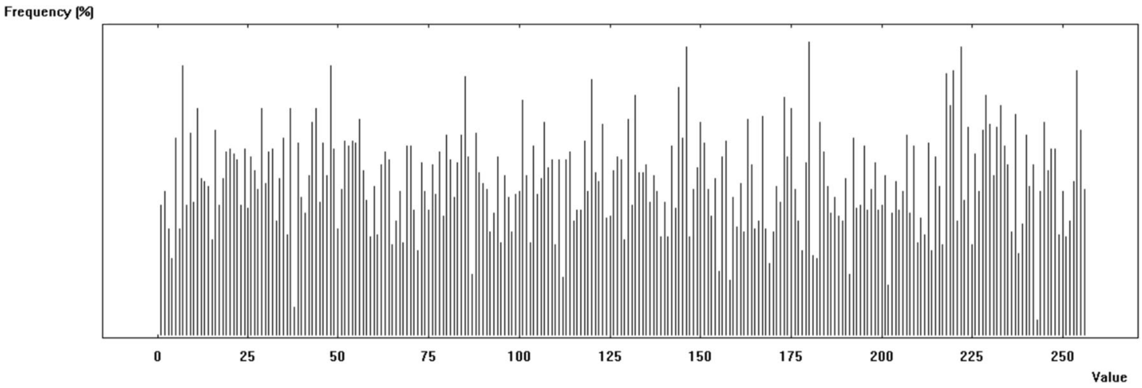

Fig. 4 Character frequency of plain intraoral file by proposed encryption

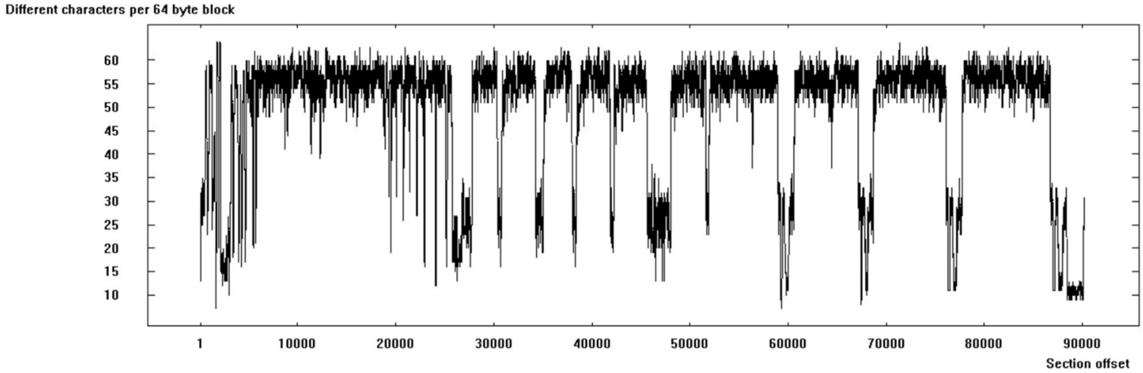

Fig. 5 Floating frequency of plain intraoral file

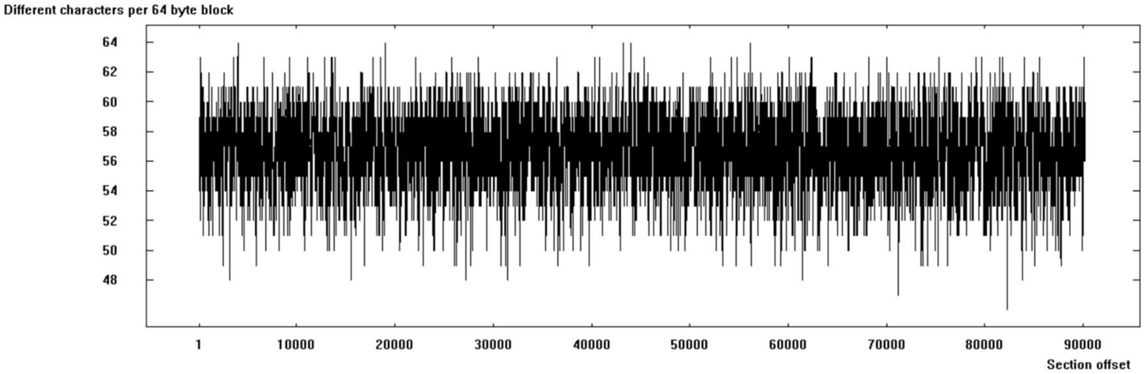

Fig. 6 Floating frequency of plain intraoral file by proposed encryption

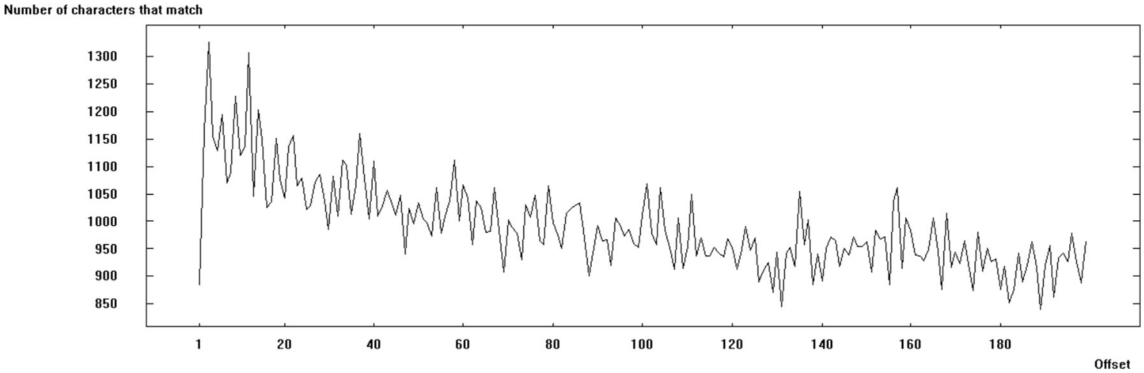

Fig. 7 Autocorrelation of plain intraoral file

be found in Fig. 8. Enhanced autocorrelation has been observed in this proposed technique.

5.4 Performance comparison with classical encryption

As we know that IDEA algorithm works on 64 bits plaintext to 64 bits cipher text by using 128 bits secret key, but the proposed technique offers the same on n bits plaintext to n bits cipher text with key generated by the perceptrons at the patient and dentist end. The most powerful linear cryptanalysis attack was done on the DES algorithm due to availability of known plaintext. The proposed technology is fully dependent on the intraoral files of different patients, which are by far different from one another. RC5 is basically word oriented encryption where the length of the word may be 16 bits, 32 bits, 64 bits. The proposed technique allows generating a header addition to each partial share. Through this strategy, the better performance of the proposed technique has been represented [32].

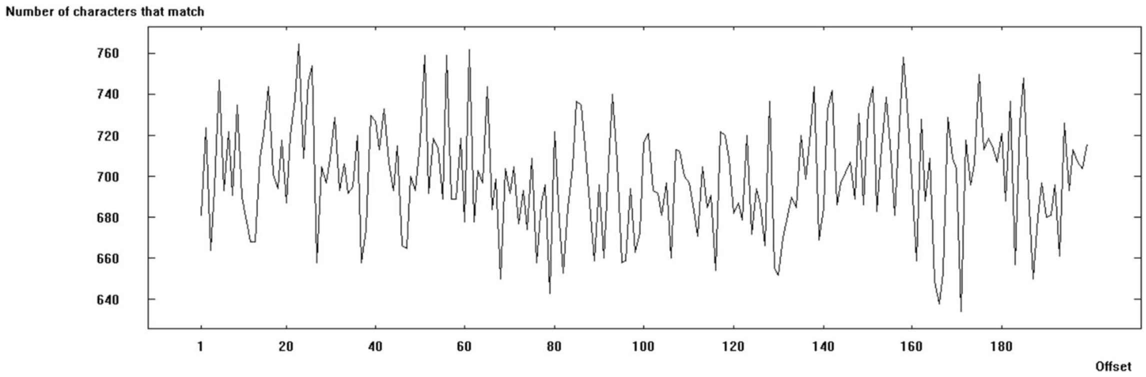

Fig. 8 Autocorrelation of plain intraoral file by proposed encryption

6 Conclusions

In this Telecare E-Health field, patients' medical data can be compromised by different types of attacks on the system. To ensure that this paper has proposed an efficient and secured technique to transmit the intraoral data. Symmetric key has been used her which is generated by the perceptron neural machine. The advantage is that there needs no secret key exchange between the patients and the dentist for symmetric cryptography. Statistically, the proposed technique has been shown as an efficient technique for data transmission in the sector of Telecare dental E-Health.

Acknowledgement All the authors do immensely thank Dr Sukriti Ghosal, Principal, M.U.C. Women's College, Burdwan, India, for his active and moral support.

Compliance with ethical standards

Conflict of interest The authors declare that there is no conflict of interest for this publication.

References

1. Kahate A (2010) Cryptography and network security, 2nd edn. Tata McGraw Hill, New York
2. Mullai A, Mani K (2020) Enhancing the security in RSA and elliptic curve cryptography based on addition chain using simplified Swarm Optimization and Particle Swarm Optimization for mobile devices. Int J Inf Technol. https://doi.org/10.1007/s41870-019-00413-8
3. Das A, Veni Madhavan CE Public-key cryptography: theory and practice. Pearson Education (in press)
4. Tajammul M, Parveen R (2020) Auto encryption algorithm for uploading data on cloud storage. Int J Inf Technol 12:831–837
5. Bhowmik A, Dey J, Sarkar A, Karforma S (2019) Computational intelligence based lossless regeneration (CILR) of blocked gingivitis intraoral image transportation. IAES Int J Artif Intell (IJ-AI) 8(3):197–204
6. Michael Rosen-Zvi IK, Kinzel W (2002) Cryptography based on neural networks—analytical results. J Phys A 47(35):707–713
7. Hamid Y, Shah FA, Sugumaran M (2019) Wavelet neural network model for network intrusion detection system. Int J Inf Technol 11:251–263
8. Sarkar A, Dey J, Bhowmik A, Mandal JK, Karforma S (2018) Energy efficient secured sharing of intraoral gingival information in digital way (EESS-IGI). In: Mandal J, Sinha D (eds) Social transformation—digital way. CSI 2018. Communications in Computer and Information Science, vol 836. Springer, Singapore. https://doi.org/10.1007/978-981-13-1343-1_49
9. Sarkar A, Dey J, Chatterjee M, Bhowmik A, Karforma S (2019) Neural soft computing based secured transmission of intraoral gingivitis image in E-Health. Indones J Electr Eng Comput Sci 14(1):178–184
10. Petersen PE, Bourgeois D, Ogawa H, Estupinan-Day S, Ndiaye C (2005) The global burden of oral diseases and risks to oral health. Bull World Health Organ 83:661–669
11. Ide M, Papapanou PN (2013) Epidemiology of association between maternal periodontal disease and adverse pregnancy outcomes—systematic review. J Periodontol 84:S181–S194
12. Yu Y-H, Chasman DI, Buring JE, Rose L, Ridker PM (2015) Cardiovascular risks associated withincident and prevalent periodontal disease. J Clin Periodontol 42:21–28
13. Li X, Kolltveit KM, Tronstad L, Olsen I (2000) Systemic diseases caused by oral infection. Clin Microbiol Rev 13:547–558. https://doi.org/10.1128/CMR.13.4.547-558.2000
14. Wade WG (2013) The oral microbiome in health and disease. Pharmacol Res 69:137–143
15. Batchelor P (2014) Is periodontal disease a public health problem? Br Dent J 217:405–409
16. Ryan ME, Carnu O, Kamer A (2003) The influence of diabetes on periodontal tissues. J Am Dent Assoc 134:34S-40S
17. Schätzle M, Löe H, Bürgin W, Anerud A, Boysen H, Lang NP (2003) Clinical course of chronicperiodontitis. I. Role of gingivitis. J Clin Periodontol 30:887–901
18. Boyd D, Crawford K (2012) Critical questions for big data: provocations for a cultural, technological, and scholarly phenomenon. Inf Commun Soc 15(5):662–679
19 Kacfah Emani C, Cullot N, Nicolle C (2015) Understandable big data: a survey. Comput Sci Rev 17:70–81
20. Alexander FJ, Hoisie A, Szalay A (2011) Big data [Guest editorial]. Comput Sci Eng 13(6):10–12 (**Article ID 6077842**)
21. Pu X, Chen SX, Yu XP, Zhang L (2018) Developing a novel hybrid biogeography-based optimization algorithm for multilayer perceptron training under big data challenge. Hindawi Scientific Programming, Programming Foundations for Scientific Big Data Analytics (Special Issue), vol 2018, p 7

22. Hitzler P, Janowicz K (2013) Linked data, big data, and the 4th paradigm. IOS Press, Amsterdam
23. Fine TL (1999) Feedforward neural network methodology. Inf Sci Stat 12(4):432–433
24. Hassoun MH (1995) Fundamentals of artificial neural networks. MIT Press, Cambridge
25. Deng CW, Huang GB, Xu J, Tang JX (2015) Extreme learning machines: new trends and applications. Sci China Inf Sci 58(2):1–16
26. Odom RC, Paul P, Diocee SS, Bailey SM, Zander DM, Gillespie JJ (1999) Shaly sand analysis using density-neutron porosities from a cased-hole pulsed neutron system. In: Proceedings of the SPE rocky mountain regional meeting, Gillette, Wyoming
27. Mat Isa NA, Mamat WMFW (2011) Clustered-hybrid multilayer perceptron network for pattern recognition application. Appl Soft Comput 11(1):1457–1466
28. Hornik K, Stinchcombe M, White H (1989) Multilayer feedforward networks are universal approximators. Neural Netw 2(5):359–366
29. Mirjalili S, Mirjalili SM, Lewis A (2014) Let a biogeography-based optimizer train your multi-layer perceptron. Inf Sci 269:188–209
30. Patel K (2019) Performance analysis of AES, DES and Blowfish cryptographic algorithms on small and large data files. Int J Inf Technol 11:813–819. https://doi.org/10.1007/s41870-018-0271-4
31 Dey J, Bhowmik A, Sarkar A, Karforma S (2019) Privileged authenticity in reconstruction of digital encrypted shares. IAES Int J Artif Intell (IJ-AI) 8(2):175–180
32. Bhowmik A, Karforma S, Dey J, Sarkar A (2020) A Defensive approach against mathematical cryptanalysis using symmetric key and fuzzy based session key. J Math Sci Comput Math 1(3):272–299