Indonesian Journal of Electrical Engineering and Computer Science
Vol. 14, No. 1, April 2019, pp. 178~184
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v14.i1.pp178-184

Neural soft computing based secured transmission of intraoral gingivitis image in e-health care

Arindam Sarkar[1], Joydeep Dey[2], Minakshi Chatterjee[3], Anirban Bhowmik[4], Sunil Karforma[5]
[1]Department of Computer Science & Electronics, Ramakrishna Mission Vidyamandiara, Belur Math, India
[2,3]M.U.C. Women's College, B.C. Road, India
[4]Department of Computer Application, Cyber Research & Training Institute, India
[5]Department of Computer Science, The University of Burdwan, India

Article Info

Article history:

Received Jul 3, 2018
Revised Oct 14, 2018
Accepted Dec 30, 2018

Keywords:

Gingivitis
Secret shares
Tree parity machine

ABSTRACT

In this paper, a key based soft computing transmission of intraoral gingivitis image has been proposed without the exchange of common key in between the nodes. Gingivitis has been a type of periodontal disease caused due to bacterial colonization inside the mouth, having the early signs of gum bleeding and inflammations in human beings. In E-health care strata, online transmission of such intraoral images with secured encryption technique is needed. Session key based neural soft computing transmission by the dentists has been proposed in this paper with an eye to preserve patients' confidentiality factor. To resist the data distortion by the eavesdroppers while on the transmission path, secured transmission in a group of tree parity machines was carried out. Topologically same tree parity machines with equal seed values were used by all users of that specified group. A common session key synchronization method was applied in that group. Intraoral image has been encrypted to generate multiple secret shares. Multiple secrets were transmitted to individual nodes in that group. The original gingivitis image can only be reconstructed upon the merging of threshold number of shares. Regression statistics along with ANOVA analysis were carried out on the result set obtained from the proposed technique. The outcomes of such tests were satisfactory for acceptance.

Corresponding Author:

Arindam Sarkar,
Department of Computer Science & Electronics,
Ramakrishna Mission Vidyamandiara,
Belur Math, Howrah -711202, WB, India.
Email: arindam.vb@gmail.com

1. INTRODUCTION

Dental care contributes a lot towards a healthy lifestyle of a person. Early signs of inflammatory gums with redness, soreness and occasional bleeding, indicates the occurrence of the periodontal disease called Gingivitis [1]. Gingivitis is the first stage of gum disease. According to ADA (American Dental Association), early detection of the disease is essential to prevent harm to teeth and gums. There are some common warning signs which are as follows:

a. Inflammations of the gums: Gums are red, swollen and sensitive to touch. Deposition of plaque [(viz. an invisible, sticky film composed mainly of bacteria) which if not removed, hardens at the gum line to form calculus or tartar] at the line of gum destroys the gum tissue and increases sensitivity.
b. Teeth appear longer: This happens due to recession of the gum line due to deposition of plaque.
c. Appearance of periodontal pockets: Spaces are created between a tooth and gum where bacteria do colonize due to loosening of the gum tissue.

d. Bad breath: A warning sign of gingivitis is chronic bad breath.
e. Formation of pus between the tooth and gum.

Figure 1. Patient suffering from Gingivitis

When the same key is used for both encryption and decryption purpose, then it is called symmetric key algorithms [2], [3]. In asymmetric key algorithms, a pair of keys i.e. a public key and a private key are used for encryption and decryption process respectively [4]. The idea of a private and public key were proposed by Whitfield Diffie and Martin Hellman in a ground breaking published paper in 1976 [5]. In public-key cryptography, the key generation and key exchange are the significant concerned issues.

1.1. Related Survey

Gingivitis is caused primarily due to colonization of bacteria. The deposition of plaque on the surface of teeth leads to gingivitis due to lack of dental proper care. Toxins which are produced, if daily brushing and flossing properly not done, leads to periodontal gingival swelling. If untreated early, it may develop to major irreversible periodontal diseases. Endocrinal hormonal variations cause gingivitis to occur too. The levels of estrogens while attaining puberty, pregnancy, periods, and menopause, drifts over the certain time frame. Such conditions activate the gingivitis disease in human body.

1.1.1 Survey on Secret Sharing

Secret Sharing scheme is a technique used by the sender to sharing a data among a group of n number of receivers. The original secret data can be reconstructed if only if the threshold value of partial shares are merged together. The individual partial encrypted shares are almost meaningless to the intruders. The technique with low space efficiency proposed by Blakley [6] is on hyper plane geometry. The idea is that secret is a co-ordinate value with respect to k- dimensional space in such a way that n numbers of secret shares are affine hyper planes which passes through secret point. The general equation of hyper planes in a k-dimensional space is a linear equation as given below.

$$p1\,x1 + p2\,x2 + p3\,x3 + \cdots \ldots + pk\,xk = q \quad (1)$$

1.1.2 Survey on Tree Parity Machine

A forward feeding artificial neural network having input, hidden and output layer is known as tree parity machine (TPM) [7], [8] as shown in Figure 2. The number of input, hidden and output neuron(s) is $K * N$, K and 1 respectively. The identical inputs $xij \in \{-1, 0, +1\}$ are fed into the participating TPMs. The hidden units are randomly assigned a weight vector wij within the range $-L\ to\ +L$ where L denotes an integer. Each hidden neuron unit generates an intermediate output as, $\sigma i = SGN([\sum_{j=1}^{N}((\text{wij}) * (wij))]$ where $SGN(P)$ returns $1, 0$ and -1 for $P > 1, P = 0\ and\ P < -1$ respectively.The output of a TPM is calculated as product of all hidden units outputs as $\Gamma = \prod_{i=1}^{K}(\sigma i)$

1.2. Problem Specifications

While transmitting such medical data over the public channel, there is a high chance of different types of attacks. It may be simple attacks, man in the middle attacks, brute force attacks, geometric attacks, etc. The classical algorithms when applied on the medical data may disclose the patients' confidential information. The existing system [9, 10] has several disadvantages. A few of them are listed as follows.

a. If the key is compromised while exchanging it, then the entire message will be revealed at once [11].
b. Once a key is leaked by the intruders, it would be valid throughout the sessions. Thus, secret data is available to the intruders.

c. In case of channel compromised, the entire secret data is transferred in a single channel would be leaked.
d. The secret data cannot be regenerated when the entire channel or key is lost or abrupt.
e. Changes in the bits of partial shares of data which leads to changes in the pattern of the data.
f. Distorted image transmission promotes to wrong treatment actions.

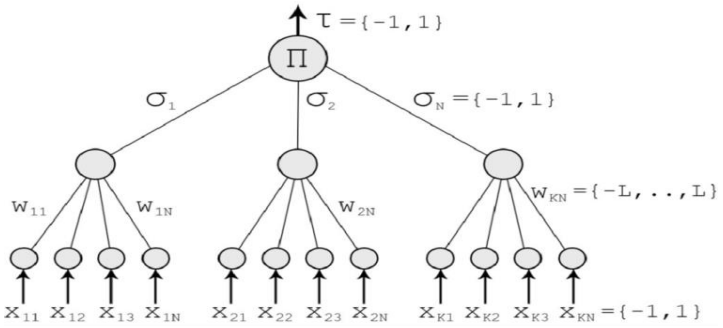

Figure 2. A sample of TPM

1.3. Solution Approach

A group sharing concept of {n, k: k < n} pair is implemented in this paper where n and k represents number of recipients and threshold number of recipients for reconstruction respectively. To treat the patients in a better way, opinions from different dentists are necessary. The intense flavor of group sharing is that original data will be partially distributed to n number of recipients. To reveal the actual information, minimum k number of recipients must agree to regenerate the original data. A masking technique applied to generate a binary mask matrix, which is used to encrypt the original information to generate n number of partial shares.

Synchronization is achieved by all the participating users after a finite number of iterations. The same pseudo random number generated by the same seed logic is fed into the input neurons of each tree parity machines. Discrete random weights within a certain limit are assigned to the hidden neurons. By training the tree parity machines using learning rules, TPMs adjust their hidden weight vector to synchronize themselves fully. Thus, equal weight vector is generated at all the nodes without exchanging the actual session key. Gingivitis image will be thus encrypted using this session key and furthermore to be transmitted to n number of recipients.

2. PROPOSED METHODOLOGY

The proposed technique minimizes the limitations stated in the above section 1.1. Here, gingivitis image of the patient is converted into binary matrix. Then a mask matrix of two dimensional order is created which indeed generate the encrypted partial shares of the image by performing successive bitwise XOR operation. Hence n numbers of partial shares are generated for corresponding n number of experts. All participating nodes are using the same architecture of neural networks to synchronize the session key. The key idea behind to implement the TPM is not to exchange the actual session key for the transmission purpose. The weight vectors corresponding to same TPM output will be trained by the learning rules. The same procedure tuning of weight vector is simultaneously executed by all the assigned TPMs in the group. Once a session key generated, then using that data can be encrypted and transmitted to the desired destination TPMs. Finally, those n numbers of partial shares are transmitted to n numbers of recipient TPMs.

Proposed Algorithm

Requirement(s): Intraoral image (I1.JPG) & Pseudo random seed value(S1)
Input(s): Total no. of recipients (n), No. of threshold (k) shares & Architecture of TPM.
Output(s): (n) number of secret partial shares of gingivitis image.
Method(s): Intraoral image is transformed into binary matrix and a mask matrix is designed. Then bitwise XOR operation is performed between binary image matrix and mask matrix to generate partial secret shares. A common session key generated without exchange for all TPMs before encrypting the shares by that key.

{/* Image to Binary Matrix Convertion*/}
for i= 0 to img_width
  for j= 0 to img_height
    Bin_Matrix[i][j] = $Convert2BinaryMatrix$(I1.JPG)
  end for
end for
{/* Mask Generation*/}
for $i = 1$ to $n_{C_{k-1}}$ do
  for $j = 1$ to n do
    $Mask[n_{C_{k-1}}][n] = CreateMask(n, k)$;
  end for
end for
{/*Bitwise XOR operation on I1.JPG with Mask matrix to generate n number of partial secret shares*/}
Set $v = 1$ and $z = 1$
for $i = 1$ to n do
  for $j = 1$ to $n_{C_{n-k}}$ do
    $Share[i][j] = Mask[i][j] \,\text{¦¦}\, Bin\_Mat[v][z]$
    $increment\ j$
    $increment\ v$
    $increment\ z$
  end for
  $increment\ i$
end for
{/*Session Key Generation by TPMs*/}
{/*Identical Input Feeding*/}
for $i = 1\ to\ n$ do
  for $i = 1$ to $K * N$ do
    for j = $1\ to\ i$ do
      $xij \leftarrow InputSequence(Seed\ S1)$
      $increment\ j$
    end for
    $increment\ i$
end for
{/*Weight Vector Initialization*/}
for $i = 1$ to n do
  for $i = 1$ to K do
    for j = 1 to i do
      $w[i, j] = PseudoRandomNumber(-L, +L)$;
      $increment\ j$
    end for
      $increment\ i$
  end for
end for
{/*Hidden Units Output Calculation*/}
for $i = 1$ to n do
  for $j = 1$ to K do
    PI$[i] = SGN(xij * wij)$
    $increment\ i$
  end for
end for
{/*TPM Output Calculation*/}
for $j = 1$ to n do
  for $i = 1$ to K do
    Tj= $\prod_{i=1}^{K}(PI\ i)$
    $increment\ i$
  end for
end for
{/*Learning by TPMs*/}

for $i = 1$ to n do .
  for $j = (i + 1)\ to\ n$ do
    if $(Ti = Tj)$ Then
      $Call\ LearningRules$
    end if
    $increment\ j$
  end for
  $increment\ i$
end for
Ready n shares and they are encrypted by common session key wij

3. RESULTS AND INTERPRETATION

This proposed technique can be used in secured image encryption [12] and authentication in wireless network [13]. In Table 1, data has been collected on the basis of two out of three parameters of the tree parity machines were kept static and fluctuating the third parameter. The value of number of input neurons (N) is 5 and number of hidden neurons (K) is 10, and varying the range of weight vector from [2], [10] and the number of successful iterations are noted for synchronization. The key aspect of this observation is sequence of the number of iterations needed is random in nature. By increasing the range value of the weight vector, the number of iterations either increases or decreases accordingly with no direct proportionality with range value. The topology of the TPM becomes more complex with rise in either of the input parameters. Trial testing on the different sets of TPMs performed in parallel fashion within the session period by the intruders would be almost impossible. Due to randomness in the key length independent of the input and hidden neurons, session key synchronized in that particular group of TPMs would be tough to detect by brute force analysis. Thus, it shows a positive aspect towards our proposed technique.

Table 1. Set of observations in TPM (N=5, K=10 & L< 8)

Column 1 Input Nodes(N)	Column 2 Hidden Nodes (K)	Column 3 Range of weight = (L)	Column 4 No. of successful Iterations (Itr)
5	10	2	182
5	10	3	272
5	10	4	1750
5	10	5	4206
5	10	6	1396
5	10	7	3158

Hence, to predict the exact number of iterations needed to synchronize by the TPMs in the specified group would be very difficult by the intruders. Some statistical values were derived from Table 1, as listed in the following Table 2.

Table 2. Some Statistical Calculations on Table 1

Parameters	Values
Standard Deviation (Column 4 of Table 1)	1596.68
Average Deviation (Column 4 of Table 1)	1236.4444
Correlation Coefficient (Column 3, Column 4: of Table 1)	0.693244
Quartile 1 (Column 4 of Table 1)	553
Quartile 2 (Column 4 of Table 1)	1573
Quartile 3 (Column 4 of Table 1)	2806
Kurtosis (Column 4 of Table 1)	1.0410845

Table 3 contains the regression statistics of range value of the weight vector and number of iterations needed to synchronize. Standard error observed is low i.e. the set of observations are consistent in nature. The coefficient of determination is 0.48, which is acceptable for the proposed technique. By keeping the number of input and hidden neurons constant, we have calculated multiple regression of range of the random weight vector and number of successful iterations needed to synchronize in group, and the multiple R value is 0.69, which is satisfactory to an extent. From Table 4 and 5, we have calculated analysis of variance, and corresponding F value is 3.701.

Table 3. Regression Statistics of Column 3 & 4 of Table 1

Parameters	Values
Multiple R	0.693244037
R Square	0.480587295
Adjusted R Square	0.350734119
Standard Error	1.507458319
Observations	6

Table 4. ANOVA Observations of Column 3 & 4 of Table 1

Parameter	df	SS	MS	F	Significance (F)
Regression	1	8.410277666	8.410277666	3.701005314	0.126716082
Residual	4	9.089722334	2.272430584		
Total	5	17.5			

Table 5. Error Observations of Column 3 & 4 of Table 1

Parameters	Coefficients	Standard Error	t Stat	P-value	Lower 95%	**Upper 95%**	Lower 95.0%	Upper 95.0%
Intercept	3.015705938	0.986922957	3.055665001	0.037818257	0.275568525	5.755843351	0.275568525	5.755843351
X Variable 1	0.000812273	0.000422223	1.923799707	0.126716082	-0.000360007	0.001984553	-0.000360007	0.001984553

Table 6 and 7 contains the ANOVA on single factor for range value of the weight vector and number of successful iterations. Here, ANOVA (F) is 9.745893; this is significant value and p value is 0.01 which is highly acceptable for our proposed works. The total SS and df are 21069710 and 9 respectively.

Table 6. Summary of ANOVA (Single Factor Column) of Column 3 & 4 of Table 1

Groups	Count	Sum	Average	Variance
2	5	25	5	2.5
182	5	10782	2156.4	2374599

Table 7. Observations of ANOVA (Single Factor Column) of Column 3 & 4 of Table 1

Source of Variation	SS	df	MS	F	P-value	F criteria
Between Groups	11571305	1	11571305	9.745893	0.014189	5.317655
Within Groups	9498405	8	1187301			

4. CONCLUSION

Based on the proposed technique of group secret transmission of the gingivitis image preceded by the session key synchronization of the TPMs with topology, N= 5, K=10, and 2<=L<8, the statistical results show better performance. The positive correlation coefficient has been generated between the L value and successful number of iterations. Hence, it determines more acceptability factor of our technique. The corresponding F value obtained from the analysis of variance from the data set of observations is also satisfactory. In the domain of E-health service, such confidential secret online communication is needed where patients' information can be kept hidden. Intruders are not capable enough to reveal the entire information during message transmission.

5. FUTURE SCOPE OF WORK

Future plan of the proposed methodology is to implement optimization techniques to enhance the transmission time in any suitable field of wireless transactions.

REFERENCES

[1] Sfyroeras G S, Roussas N, Saleptsis V G, Argyriou C, Giannoukas A D. Association between periodontal disease and stroke. *Journal of Vascular Surgery. 2012*; 55(4): 1178-1184.

[2] Ahmad, J.I. , Din, R. , Ahmad, M., Review on Public Key Cryptography Scheme-Based Performance Metrics, *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)* Vol. 12, No. 1, October 2018, pp. 386-392.

[3] Kahate A. Cryptography and Network Security. 2nd edition: Tata McGraw Hill. 2010.

[4] Diffie W., Hellman M. *Multi-user cryptographic techniques*. AFIPS. New York. 1976; 109-112.

[5] Shamir A. How to share a secret. *Communications of the ACM. 1979;* 22(11): 612-613.

[6] Blakley G R. *Safeguarding Cryptographic Keys*. AFIPS International Workshop on Managing Requirements Knowledge.1979; 313 – 317.

[7] Wolfgang Kinzel, ldo Kanter. *Neural Cryptography*. Neural Information Processing (ICONIP 02) . Singapore. 2002.

[8] Wolfgang Kinzel, ldo Kanter. *Interacting Neural Networks and Cryptography*. Advances in Solid State Physics. Berlin. 2002; 42: 383.

[9] Mislovaty R, Perchenok Y, Kanter I, Kinzel W. Secure Key-exchange Protocol with an absence of injective functions. Phys. Rev. E. 66:066102. 2002.

[10] Ruttor A, Kinzel W, Naeh R, Kanter I. Genetic attack on Neural Cryptography. Phys. Rev. E, 73(3):036121. 2006.

[11] Sarkar A, Mandal J K. Cryptanalysis of Key Exchange method using Computational Intelligence guided Multilayer Perceptron in Wireless Communication (CKEMLP). *Advanced Computational Intelligence: An International Journal (ACII)*. 2014; 1(1): 1-9.

[12] H. Ali-Pacha, N. Hadj-Said, A. Ali-Pacha, M. Mamat, and M. A. Mohamed, "An Efficient Schema of a Special Permutation Inside of Each Pixel of an Image for its Encryption," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 11, no. 2, 2018.

[13] Choi, Younsung. "Cryptanalysis on Privacy-aware two-factor Authentication Protocol for Wireless Sensor Networks". *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, Vol. 8, no. 2, pp. 296-301, 2017.