Computational intelligence based lossless regeneration (CILR) of blocked gingivitis intraoral image transportation

Anirban Bhowmik[1], Joydeep Dey[2], Arindam Sarkar[3], Sunil Karforma[4]
[1]Department of Computer Applications, Cyber Research &Training Institute, Burdwan-713101, India
[2]Department of Computer Science, M.U.C Women's College, B.C. Road, Burdwan-713104, India
[3]Department of Computer Science & Electronics, Ramakrishna Mission Vidyamandira, Belur Math -711202, India
[4]Department of Computer Science, The University of Burdwan, Burdwan-713104, India

Article Info

Article history:

Received Feb 9, 2019
Revised Mar 6, 2019
Accepted May 9, 2019

Keywords:

Entropy
Frame Format Orientation
Lossless Data Property
Mask Matrix
Secret Intraoral Image

ABSTRACT

This paper presented that an intraoral image has been wrapped during wireless transportation with an encryption tool with an added essence of lossless regeneration property. Threshold based cryptographic transportation has provided the construction of reliable and robust medical data communication system. The accumulation of threshold shares only would result to the formation of the intraoral gingivitis image at the receivers' end. The proposed technique dealt with the generation of n number of partial shares by creating a unique frame structure by the dentist / physician. Additional feature has been proposed on the computational lossless transportation.The existing techniques cause a high computational complexity. The proposed technique ensured the lossless regeneration property while blocked gingivitis image sharing. Filling of bits have been incorporated to ensure the static sized homogeneous blocks of intraoral gingivitis image. A graphical masking method had been deployed, followed by successive decryption procedure on minimum threshold shares that ensure lossless data regeneration. This can guide the dental treatment with enhanced accuracy. Different types of statistical testing like entropy analysis and histogram analysis confirms the exhibition of authenticity, confidentiality, and integrity of our proposed technique.

Corresponding Author:

Joydeep Dey,
Department of Computer Science,
B.C. Road, Post Rajbati,
Burdwan, West Bengal, India, PIN – 713104.
Email: joydeepmcabu@gmail.com

1. INTRODUCTION

The key aspect is to channelize an online transmission of data through secured procurement by applying mathematical hardness. The effective and reliable data communications using cryptography tools [1-3] is a significant issue in modern technological era. There are so many emerging cryptography techniques [4]. Compromising the recipient leads to leakage of data. In medical domain of data communication, secured transmission of data is necessarry. An effective solution is to distribute the medical image into different shares along with encryption algorithm. The key idea behind such technique is to a $\{n, k : k \leq n\}$ threshold based information sharing between the n numbers of recipients. To restructure the original image, k numbers of threshold shares are required. If the minimum numbers of recipients do not agree, then by no means the information can be revealed.

A function sharing problem is one of the shortcomings of perfect secret sharing scheme where function computation [5, 6] is distributed according to secret sharing scheme such that the individual user computes the shared parts and then the partial result can be combined to yield the final result without disclosing the individual secrets. Various function sharing protocols are there such as Shamir Secret Sharing [7] based on polynomial interpolation, Blakley's Secret Sharing based on hyper plane geometry [8] and Asmuth-Bloom Secret Sharing based on Chinese remainder theorem[6]. In dental professional, it may be assumed as if an image M is splitted into p number of shares with the necessary condition that minimum t numbers of shares are to be merged to regenerate the original image. Thus, the proposed methodology sustains the lossless join decomposition during an intraoral image transmission by a medical professional. Periodontal disease [9] is a type of gum disease with more gum swelling which may affect our jaw bones and related nerves and tissues. Bacteria biofilms are a major reason behind the damage of gums, cementum covering upon roots, alveolar nerves, periodontal ligaments, etc. Gingivitis is a type of periodontal disease which is very common and reccuring in humans. Following Figure 1 shows gingivitis affected intraoral image.

Figure 1. An intraoral image showing gingivitis

Literature survey

Gingivitis and its causes

The simple meaning of periodontal is "perio" that means around and "dontal" which means teeth. In other words, periodontal disease is a type of gum disease caused by the acute colonization of bacteria. The common sysmptoms are with more gum swelling and soreness, which may even damage the jaw bones and corresponding nerves and tissues. Gingivitis and periodontitis [9] are the most common bacterial infections in the human craniofacial area. The sedimentation of plaque on the surface of teeth leads to gingivitis due to irregular and improper dental care. When untreated early, it may emerge to irreversible periodontal diseases due to secretation of harmful toxins.

Related works on secret sharing

Shamir's Secret Sharing Scheme [7] is mathematically based on $\{n, k : k <= n\}$ threshold system, where n and k represents the number of receivers and threshold value respectively. Here accumulation of $(k-1)$ degree polynomial is necessary. So, polynomial function is of the order $(k-1)$ is constructed by the following (1).

$$f(x) = (p_0 + p_1x^1 + p_2x^2 + \dots + p_{k-1}x^{k-1}) \mod m \quad (1)$$

where p_0 is the secret and m is a prime number and the remaining coefficients are taken randomly from the secret.

Blakey has used geometry to solve secret sharing problem [8]. The secret data is a point that lies on a $k-$dimensional space and corresponding n shares are a affine hyper planes that intersect here. The set solution $y = (y_1, y_2, y_3, y_4, \dots, y_k)$ to an equation $p_1y_1 + p_2y_2 + \cdots + p_ky_k = b$ forms an affine hyper plane. The secret the intersection point is calculated by finding the intersection of any k of these hyper planes. Above stated secret sharing schemes are considered as a perfect secret sharing scheme because accumulation of (k-1) shares doesn't expose any data.

Problem findings

Gingivitis [9] is a significant common periodontal disease which affects the periodontum and related human organs. It is a frequent and recurring disease in rural areas. Gingivitis is caused by the bacteria infection inside the mouth. In such remote areas there exists a lack of infrastructure with medical perspective. The availability of expertise personnel such as dentists, physicians, anaesthetics, paediatricians, dieticians, etc is very rare in such remote areas. In most of the rural areas, there are no such reputed X–Ray clinics, pathological laboratories, medical support clinics, etc. The patients belonging from these areas suffer a lot. Since they do not get particular expert opinion due to various reasons, their disease gets untreated and further damage leads to irreversible states of the periodontum. Also in remote villages no such expert persons are available who are capable of observing the symptoms of the gingivitis efficiently. That is no expert visualization of the disease. If such expert persons are available in remote areas, then they could physically verify the affect body part and collect the specified symptoms of gingivitis from patients, and hence would provide inputs to the existing medical expert system. If these persons provide invalid and non specific inputs to the expert system, then wrong diagnosis of the disease will be generated. Thus the treatment procedure would be in wrong path to follow which is not at all desirable. Such a vital gingivitis disease needs proper medical diagnosis in appropriate time so that the patients get suitable medical advice from expert dentists and physicians. For this reason an online secured transmission technique is needed for transmitting various intraoral images to various dentists or physicians for their expert opinion by preserving the lossless data property.

Solution strata

Secret sharing [7, 8] on the intraoral images has been proposed for positive treatment in the medical domain. Session key has been generated using a hash function in this technique to facilitate the randomness. Intraoral images are being blocked into homogeneous entities before wrapped by the proposed encryption frame format. Partial shares are generated with the propsed mask matrix with the added flavour of lossless computation intelligence. Detailed explanations of the proposed technique over the dental treatment have been described in the later sections.

2. PROPOSED METHODOLOGY

To substantiate the problem findings specified in above section, a mask based encryption technique [10] have been applied. An image will be divided into several partial parts, out of which minimum threshold number of shares are mandatory to regenerate the original image without any loss of integrity. Joining of minimum partial shares accomplishes the lossless joining of data shares. The objective of this methodology is to obtain a lossless and secured transmission of intraoral image for the greater benefits of the community. Even from remote locations, expert opinion can be easily available for myriad dental diseases. Such an innovative move may evolve as a protocol in the well secured telemedicine sector [11, 12].

2.1. Proposed algorithm: CILR of intraoral Image transportation

Requirement(s): $Master\ Key\ of\ Sender\ (Mk), Source\ Image\ (say\ S1.JPG\ )$

Input(s): $n, k\ :\ Number\ of\ recipients$ & $Threshold\ number\ respectively$

Output(s): $Double\ Encrypted\ partial\ shares\ of\ the\ gingivitis\ image$

{ /* Session Key Generation */ }

$$Dk[\ Size\ ]\ =\ Call\ KeyGeneration\ (\ Mk\ )$$

{ /* Mask Generation */ }

$$Mask[{}^{n}C_{k-1}][n] = Call\ MaskGen(n, k, Mask[{}^{n}C_{k-1}][n])$$

{ /* Source Image Encryption */ }

$$EF\ =\ Call\ RSA\ (\ S1.JPG\ )$$

{ /* Frame Format Orientation */ }

$$MSG[\ ]\ =\ Call\ FrameFormatOrientation(EF, Dk\ , RSA(Mk)\ )$$

{ /* Derivation of Secret Share Generation */ }

for $i =\ 0$ to $(n-1)$ do

  $EncryptedShare[i\ ]\ =\ Call\ XOR\_OPR(\ MSG[\ ]\ , Mask\ [i]\ )$

  $Increment\ i$

end for

{ /* Final Round of Encryption */ }

for $i =\ 0$ to $(n-1)$ do

  $FinalShare[i\ ]\ =\ Call\ RSA(\ EncryptedShare[i], PublicKeyPair\_Recipient[i]\ )$

  $Increment\ i$

end for

2.2. Proposed mask generation

A proposed masking technique on the pre-defined n number of shares and then to perform OR operation on the pre-defined k number of shares to regenerate the original transmitted data ensuring the lossless of data. For simplicity let us assume a secret data to be transmitted through wireless media as a sequence of binary bits which consists of 1 and 0. The secret data may be considered as an image, audio, video or any text file. The primary task is to decompose the binary file of any size into n number of shares. And on the reverse terminal end, if we perform bitwise OR operation upon k number of shares then only the original data will be reconstructed, not even upon $(k-1)$ shares [13]. Every share must have some missing bits and hence those missing bits can be replaced by $(k-1)$ shares exactly. The length of each mask can be calculated as $^{n}C_{k-1}$ i.e. $n!/(k-1)!*(n-k-1)!$. The number of missing bits and secret data bits are valued as $^{n-1}C_{k-2}$ and $^{n-1}C_{n-k}$ respectively [5].

2.2.1. Proposed mask generation algorithm

Algorithm : Proposed Mask Generation

```
Input(s): n: Number of recipients, k: threshold receipients
Output(s): Mask Matrix.
Set SIZE ← nC k
Set i ← Power ( 2 ,n )
Set J = K = 0
Set NOZ ← n-1C k-2
    While [ i >= 0 ] do
        If ( ToBinary(i).Equals( NOZ ) ) then
                        DATA [ SIZE --] ← ToBinary(i)
        End if
        Decrement i
    End while
    For i = 0 to (SIZE – 1 ) DO
        If ( (DATA[i] % 2 ).Equals( 0 ) ) then
          EVEN [ J ++] ← DATA [i]
        Else
  ODD [ K++] ← DATA [i]
        End if
    Set i ← i +1
    End for
  While ( J >= 0 || K >= 0 ) do
        FIN[k2 ++] ← EVEN[J --]
        FIN[ k2 ++] ← ODD [K --]
  End while
   If ( J!=0 ) then
    FIN[ K2…] ← COPY ( EVEN[ J … 0])
        Else
    FIN[ K2…] ← COPY ( ODD[ K … 0])
        End if
    For M = 0 to ( P – 1 ) do
        MaskMat[M][] ← Call ToBinary (FIN[M])
    End for
                MaskMat [ n] [ P] ← Call ToTranspose[ Mask[P][n] ]
```

2.3. Proposed session key generation

The dentist has been assigned with a unique transmission key (Mk) for conducting such lossless and secured channelization of any intraoral image. Initially the transmission key (Mk) is being encrypted to construct an intermediate key (Ek), which in then fed into message digest algorithm to generate the session key. The following algorithm illustrates the concept of creation of session key by the dentist.

Algorithm: Proposed Session Key Generation

```
Requirement(s): Master Key of Sender (Mk)
Input(s): Private Key pair: dentist
Output(s): Session key of fixed length
{ /* Intermediate Key Generation */ }
                Ek[ Size ] = Call RSA ( Mk )
{ /* Session Key Generation */ }
                Dk [128] = Call MD5 (Ek)
```

2.4. Proposed source image encryption

The confidentiality parameter is the most trust-worthy issue while data transmission in E-Health domain [10, 13]. The following algorithm has been used for this purpose. To encapsulate the entire information in proposed frame orientation, the initial encryption of the gingivitis image is needed. To obtain an expertise opinion from different dentists / doctors, the preservation of patients' data of any intraoral image has to be ensured. The following algorithm serves the objective of data hiding.

Algorithm: Proposed Source Image Encryption

Requirement(s): $Intraoral\ Gingivitis\ Image\ (say\ S1.JPG)$
Input(s): $Public\ key$: $dentist$
Output(s): $Encrypted\ Intraoral\ Image$
{ /* Image Encryption */ }
$EF\ =\ Call\ RSA\ (\ S1.JPG\ )$

2.5. Proposed frame format orientations

The novelty of this proposed methodology is to design a frame format. It consists of four fields: Header, Encrypted File, Message Digest, and Padding. The total length of this frame structure is dynamic. It depends on the length and type of the source image file. In true sense, the Header always contains four bits. The two most significant bits contains the size of the encrypted source file. The two least significant bits denotes 14H. The following algorithm explains the concept of creation of frame structure by the dentist.

Algorithm: Proposed Frame Format Orientation

Input(s): $Encrypted\ File\ (EF), Encrypted\ Key (EK)$ & $Message\ Digest\ Value (DK)$
Output(s): $Header\ Structure\ with\ four\ merged\ fields$
{ /* Frame Structure Generation */ }
$HS[4]\ =\ Call\ FieldsConcat\ (\ (sizeof(EF), sizeof(DK)), EF, DK, EK\ )$

2.6. Proposed derivation of secret shares

The required number of secret shares are being derived from the above stated frame format. Considering each row at a time, XOR operation has been carried out on the entire frame format by its repeated placing [14]. Homogeneity of all such blocks is maintained in this proposed methodology. In case of the ultimate block of the frame format, padding is concatenated to make it homogeneous block too. The following algorithm represents this proposed concept.

Algorithm: Proposed Secret_Share_Derivation

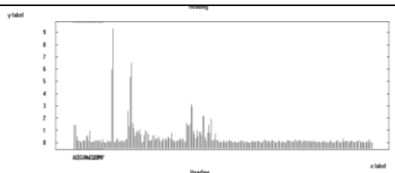
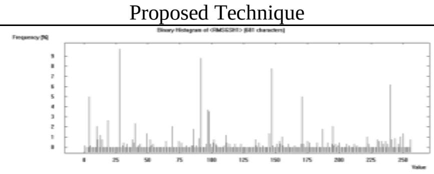
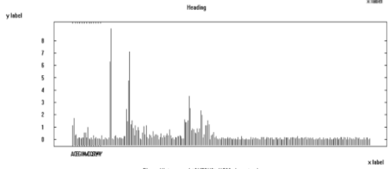
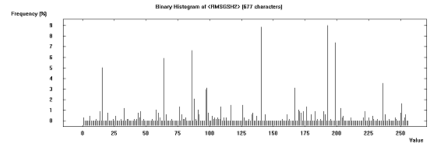
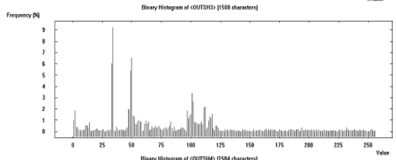
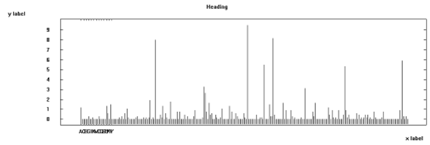
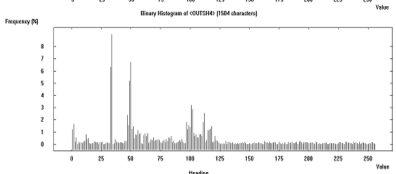
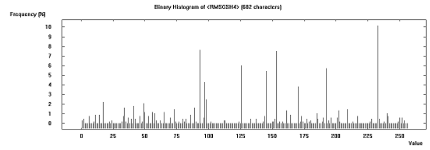
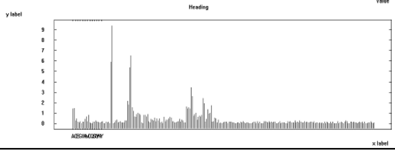
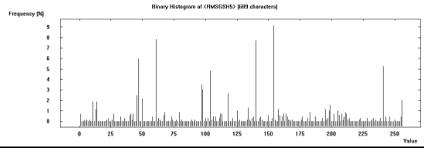
Input(s): $Mask\ Matrix$: $Mask\ [n][nCk-1\ ], Frame\ Format$: $MSG\ [\ ]$
Output(s): $'n'\ number\ of\ Secret\ Shares.$
Set shRow← get_Row (Mask[n] [${}^{n}c_{k-1}$])
for $i =\ 0$ to $(shRow-1\ )$ do
  for $j =\ 0$ to $({}^{n}C_{k-1})$ do
    $EncryptedShare\ [i][j]\ \leftarrow\ Call\ SubsequentXOR(\ MSG[\ ]\ , Mask[i][j])$
  end for
end for
for $i =\ 0$ to $(shRow-1\ )$ do
  for $j =\ 0$ to $(\ {}^{n}C_{k-1}\ )$ do
    $Share\ [i]\ \leftarrow\ Call\ LastBlockFill(\ MSG[\ ]\ , 0)$
    $EncryptedShare\ [i][j]\ \leftarrow\ Call\ SubsequentXOR(\ Share[i]\ , Mask[i][j])$
  end for
end for

3. RESULTS AND ANALYSIS OF PROPOSED METHODOLOGY

3.1. Histogram analysis

The binary histogram analysis describes how binary values of a file are distributed. It is a graphical representation of a frequency distribution. We have examined the distribution of our data, including the peaks, spread and symmetry of the cipher text and shared cipher text [15]. The peaks represent the most common values and spread represents how much our data varies. From the results in Table 1, it has been observed that the data is not skewed. The histogram of results data shows the distribution is normal and normal in shape. The above histograms of shares generated through the proposed methodology shows the distribution of data in shared file are equal which proves the encryption using symmetric key is good. Using any 'k' number of shares we can get back the encrypted file and from encrypted file it is infeasible to get an idea about symmetric key. This proves strength of our proposed scheme.The use of secret sharing scheme in our technique protects from various types of malicious attacks [14, 15].

Table 1. Histogram Comparison of plain text shares with corresponding proposed technique shares (having n=5, k=3)

Sl. No.	Secret Share ID	Histogram Plain Text	Histogram Proposed Technique
1	SECSH-1		
2	SECSH-2		
3	SECSH-3		
4	SECSH-4		
5	SECSH-5		

3.2. Entropy value analysis

Entropy is essentially randomness or unpredictability of something. In cryptography, this randomness must be supplied in the plain text message to remove the structure of the plain text message. Following Table 2 shows the entrophy values of the secret shares obtained through our proposed technique. Corresponding histogram generated for above stated Table 2 is given in the following Figure 2.

Table 2. Entropy value

Share Id	EntropyValue
SECSH-1	2.58
SECSH-2	2.59
SECSH-3	2.56
SECSH-4	2.55
SECSH-5	2.56

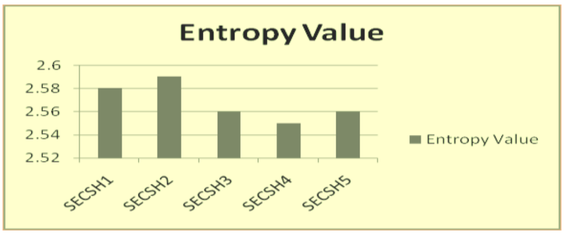


Figure 2. Bar Graph on entropy value on the proposed encypted shares.

The entrophy values which have been obtained are satisfiable to extent. In some cases a malicious attacker can guess some bits of entropy from the output of a random number generator, and there is need to ensure entropy by adding some elements that the attacker can not guess. Through cryptography, we can increase the uncertainty in the message for those who do not know the key. Plain text has entropy of zero as there is no uncertainty about it. Algorithms should take a message through a sequence of substitutions and transpositions. According to Shannon, encrypting a message will intentionally increase the message's entropy. From the above Table 2 and Figure 2, we can say that proposed technique provides randomness in plain text.

3.3. Ensurance of lossless data restructuring

The proposed technology deals with reversible encryption tool [1-2] based on merging of threshold number of shares [6-7], keeping the lossless data integrity intact. The beauty of the proposed methodology is that it holds the property of lossless join decomposition with preservation of data integrity. As a whole, computational intelligence parameter is reflected at proposed technology. It means if an intraoral image 'M' is decomposed into 'p' number of shares then the good flavour of this algorithm is if 't' number of shares i.e. minimum number of threshold shares are being joined simultaneously, then only the original image is being reconstructed. This characteristic can be explained in the following formulae A and B.

CHECKIF ($M = M1\ U\ M2\ U\ M3\ U \ldots\ldots\ldots\ldots U\ Mt$) ; lossless regeneration (A)

CHECKIF ($M \neq M1\ U\ M2\ U\ M3\ U \ldots\ldots\ldots\ldots U\ M\ t-1$) ; lost regeneration (B)

Let consider a secret intraoral image labelled as D and consider the corresponding the number of shares to be generated for decomposition be $p = 5$ and the threshold values be $t = 3$. Then the decomposed secret images are $D1, D2, D3, D4, and\ D5$ respectively. Thus, the following Table 3 shows the possible cases that can be generated.

Table 3. Lossless regeneration (n=5 & k =3)

Case ID	Union Statement	No. of participating shares >= Threshold
C#1	D = D1 U D2 U D3 U D4 U D5	5
C#2	D = D1 U D2 U D3 U D4	4
C#15	D = D1 U D3 U D5	3
C#16	D = D2 U D4 U D5	3

4. CONCLUSION

We have presented a secured key based secret sharing approach with minimal computational overhead. Here key as well as secret data is shared among set of n number of participants and from n numbers k number of participants are able to construct the original message. To the best of our knowledge this is the simplest threshold secret sharing technique, practically having minimal computational overhead during both share generation and reconstruction.

ACKNOWLEDGEMENTS

The authors acknowledge the moral and congenial atmosphere support provided by the Maharajadhiraj Uday Chand Women's College, B.C. Road, Burdwan, India (A Constituent College under The University of Burdwan, India).

REFERENCES

[1] 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.

[2] Choi Y, et al. Security enhanced user authentication protocol for wireless sensor networks using elliptic curves cryptography, *Sensors*. 2014; 14(6): 10081-10106.

[3] Jiang Q, et al. A privacy-aware two-factor authentication protocol based on elliptic curve cryptography for wireless sensor networks, *International Journal of Network Management*. 2017; 27(3).

[4] Chaudhry S A, et al., *An improved and provably secure privacy preserving authentication protocol for SIP*, Peer-to Peer Networking and Applications. 2017; 10(1): 1-15.

[5] Prabir Kr. Naskar, Hari Narayan Khan, Atal Chaudhuri, A Key Based Secure Threshold Cryptography for Secret Image, *International Journal of Network Security*, Vol.18, No.1, PP.68-81, Jan. 2016.

[6] C.Asmuth and J.Bloom, "A modular to key safeguarding*", IEEE Transaction on Information Theory*, vol.29, no. 2, pp. 208-210. 1983.

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

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

[9] 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.

[10] Arindam Sarkar,Joydeep Dey,Minakshi Chatterjee, Anirban Bhowmik, Sunil Karforma, Neural soft computing based secured transmission of intraoral gingivitis image in e-health care, *Indonesian Journal of Electrical Engineering and Computer Science*, 14(1): 178-184, April 2019.

[11] M. A. Murillo-Escobar, and et, al., A Double Chaotic Layer Encryption Algorithm for Clinical Signals in Telemedicine, *Journal of Medical Systems*, 2017 41: 59.

[12] Lin, C.-F., Shih, S.-H., and Zhu, J.-D., Chaos based encryption system for encrypting electroencephalogram signals, *Journal of Medical Systems*, 38(5):1-10, 2014.

[13] Sarkar A., Dey J., Bhowmik A., Mandal J.K., 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.

[14] Prabir Kr. Naskar, Hari Narayan Khan, Ayan Chaudhuri, Atal Chaudhuri "Ultra Secured and Authentic Key Distribution Protocol using a Novel Secret Sharing Technique", *International Journal of Computer Applications* (0975-8887) Volume 19-No.7, April 2011.

[15] Sarkar A, Mandal J K, Soft computing based Cryptographic Technique using Kohonen's Self-Organizing Map Synchronization for Wireless communication (KSOMSCT), *International Journal in Foundations of Computer Science & Technology (IJFCST)*. 2014; 4(5): 85-100.

BIOGRAPHIES OF AUTHORS

Anirban Bhowmik completed Bachelor of Science (Mathematics Honours) from Bolpur College, Bolpur, West Bengal, India and Master of Computer Application from the University of Burdwan in year 2008. He is working as an Assistant Professor in Department of Computer Applications at Cyber Research & Training Institute, Burdwan West Bengal, India since 2008. He has published five conference papers and three journal papers at reputed international journals, which are available online. His main research work focuses on Cryptography, Mathematical Modelling, and Soft Computing. He has 11 years of teaching experience at UG level.

Joydeep Dey pursed Bachelor of Computer Application (Honours) from Cyber Research & Training Institute, Burdwan, India in 2007 and Master of Computer Application from the University of Burdwan in year 2011 and he secured University First Class First Rank. He is working as Lecturer in Department of Computer Sciences at M.U.C. Women's College, Burdwan, West Bengal, India since 2011. He has published three journal papers (SCOPUS Indexed) and five international conferences papers. His main research work focuses on Cryptography and Computational Intelligence. He has 8 years and 0.5 years of teaching experience at UG and PG level respectively.

Dr. ARINDAM SARKAR is currently serving the Deparment of Computer Science & Electronics, Ramakrishna Mission Vidyamandira, Belur Math-711202, Howrah as an Astt. Professor. He has completed his Master of Computer Application (M.C.A) degree in the year of 2008 from VISVA BHARATI, Santiniketan, WB, India and he secured University First Class First Rank. In the year of 2011, Dr. Sarkar has completed his M.Tech in Comuter Science & Enggineering degree from University of Kalyani, WB, India and also secured University First Class First Rank. Dr. Sarkar has completed his Doctor of Philosophy in Engineering in the year of 2015 from University of Kalyani under the INSPIRE Fellowship Scheme of Department of Science & Technology (DST), New Delhi, India. In the year of 2016 he has secured 2nd Rank in the West Bengal College Service Commission Examination. He has more than 50 International Journal and Conference publications.

Sunil Karforma has completed his Bachelors in Computer Science & Engineering, and his Masters in Computer Science & Engineering, from Jadavpur University. He received his Ph.D. in Computer Science, and is presently Professor & Head of the Dept. of Computer Science at the University of Burdwan, India. His research interests include Network Security, E-Commerce, and Bioinformatics. He has published numerous papers in both national as well as international reputed journals and conferences.