JCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.7, Special Issue.1, Jan 2019 E-ISSN: 2347-2693

Metaheuristic Guided Secured Transmission of E-Prescription of Dental Disease

Joydeep Dey[1*], Sunil Karforma[2], Arindam Sarkar[3], Anirban Bhowmik[4]

[1]Department of Computer Science, M.U.C Women's College, B.C. Road, Burdwan, India
[2]Department of Computer Science, The University of Burdwan, Burdwan, India
[3]Department of Computer Science and Electronics, R.K.M. Vidyamandira, Belur Math, Belur, India
[4]Department of Computer Applications, C.R.T.I., Goodshed Road, Burdwan, India

[*]*Corresponding Author: joydeepmcabu @gmail.com, Tel.: +91- 9093792368*

Available online at: www.ijcseonline.org

***Abstract*—** This paper presents a novel and secured approach of transmission using the Cuckoo search metaheuristic algorithm. Dental disease is mostly caused by the colonization of the bacteria inside the oral cavity. Colonization of bacteria affects our teeth, gums, nerves, etc. Such patients are very common and to be cured appropriately. If left untreated, it may lead to severe damages inside the oral cavity. Cardiovascular and metabolic activities are also affected due to dental diseases. To transmit such information of any patient, here an encryption technique has been proposed preceded by generation of suitable key. Fittest session key has been generated by implementing the Cuckoo search metaheuristic algorithm. A mask matrix has been created for the proposed ciphering technique. Patient's E-prescription proposed by the dentist would be fragmented into multiple fragments. In this paper, serial test has been used for testing the robustness of key and test results obtained reflects the good randomness in nature.

***Keywords* -** Cuckoo Search, Fragments, Encryption

I. Introduction

With the rapid emergence in medical science domain, encryption contributes as an integral component. Symmetric and asymmetric key cryptography [1] provides a reliable and more secured data transmission. To treat a patient more precisely, dentists refer the patient's E-prescription to another dentist. To promote and encourage the dental treatment, it would be good enough to cure any dental disease without loss of generality. Dental diseases are most frequent and common in our daily life. A dentist observes and notes all the related information related to the occurrence of such oral disease. Soft copy of all the necessary observations along with his proposed treatment procedures termed as E-prescription, which would be transmitted to another dentist / doctor for better suggestions through the application of cryptographic tools. Fragmented approach on the E-prescription is used by the proposed encryption technique. Dismantling an E-prescription into multiple ciphered fragments is done at the dentist's end followed by proposed share generation tool. By authenticated requisitioning all the fragments by the receiver, do reconstruct the original file. The patients' confidentiality is highly preserved.

The generalized information, symptoms, and dentist's line of treatment procedures are recorded in the E-prescription for the dental patients.

Utilizing the idea of Cuckoo Search, the necessary private key bits are constructed. By the help of the private key bits, the E-prescription would be encrypted before transmitting to hide from the intruders.

The organization of the rest of the paper is as: Section II contains the related works. Section III contains the problem domains. The solution domain is discussed in section IV. The proposed methodology of work is described in section V. Section VI shows the obtained results and discussion. Section VII illustrates the conclusion and future scope of works, while references are tagged at the end.

II. Related Work

Ant Colony Optimization (ACO) [2, 3] is an example of genetic algorithm [4] to solve an optimization problem by imitating the ant's behaviour. It focuses on the collective behaviour of ants to perform survival tasks like transportation of food items and finding minimum path to the food sources. A chemical substance having evaporation phenomenon called pheromone, which emitted by the ants and it subsequently guides other ants to follow the same path in the interest of the food. A given ant chooses path according to the smelt quantity of pheromone with shortest paths.

Cuckoo search is a nature inspired optimization technique to solve problems [5]. The brood parasitism nature of some cuckoo species inspires to design this technique. Cuckoo lay their eggs intelligently at other bird's nest during the hatching periods, and let it to grow, if undetected by the host species. It uses Levy flight to satisfy the global convergence criteria. Levy flights are the random walks at a turn of right angle. It covers a greater area of searching.

Mask matrix generation [6-8] is a concept of deploying to cipher the data file. The idea is to decompose into n number of shares and k number of shares is good enough to regenerate the original file. The order of the matrix will be n by ${}^{n}C_{k-1}$. Each row the matrix represents a different mask which will hide certain number of bits from the source file.

III. Problem Domain

Data transmission is needed in the E-health domain of treatment. By sniffing the transmitted messages, an intruder can obtain and manipulate those messages with wrong intentions. The key generation algorithm through the random library functions may or may not be fittest in terms of randomness. Also by asymmetric key cryptography, it enables to transmit data, but in limited size and attributes. Illegal dental claims could exist in such types of dental transmission of data. This would hamper the society to a greater extent.

IV. Solution Domain

The proposed methodology provides an optimal solution to the problems addressed in the section III. Metaheuristic cuckoo search [4,5] generates true random fittest key. The larger length of data files is to be fragmented to support the fusion technique with the key. Such proposed methodology may be suitable to resist the false dental insurance.

V. Proposed Methodology

This paper presents an algorithm to generate a private key based on Cuckoo Search, which in turn is used for the ciphering purpose. A mask matrix is designed for the subsequent XOR operations, which were carried on the private key and E-prescription. This is the first round of ciphering done for the fragmentation purpose. Furthermore, a fusion between the blocks containing corresponding data and key fragments are being done.

```
Algorithm1:Proposed_Methodology
________________________________________
Input(s):Patient ID(P_id), Patient's E-prescription( EP1.PDF)
Output(s): Encrypted E-prescription with Cuckoo search generated session key.
Requirement(s): n:Number of fragments, k:Threshold fragments
// Generation of Private Key Bits
PKEY[128] ← Call CuckooSearch( KPOOL[100][128] )
// PDF to Binary File Conversion
EFILE[ ][ ] ← Call PDF2BIN( EP1.PDF )
// Masking Subroutine
MASKING[n ][$^{n}C_{k-1}$ ] ← Call MaskSub(n,k)
// Key Fragmentation
FKEY[n ][ $^{n}C_{k-1}$ ] ← Call Fragmentation (MASKING[n ][$^{n}C_{k-1}$ ], PKEY[128])
// File Fragmentation
FFILE[n ][ $^{n}C_{k-1}$ ] ← Call Fragmentation (MASKING[n ][$^{n}C_{k-1}$ ], EFILE[ ] )
// Block Generations
TFILE ← Call Block_Fusion (FKEY[n ][ $^{n}C_{k-1}$ ], FFILE[n ][ $^{n}C_{k-1}$ ] )
```

Cuckoo Search based on metaheuristic optimization technique, is used to generate the private key for encryption [9, 10]. A comparison between the cuckoo egg and the host egg is done. Optimal results egg is placed in the fittest key stream. The session key thus generated would be sent to an expert dentist. The following algorithm illustrates this proposed idea.

```
Algorithm 2: Proposed Cuckoo Search
________________________________________
Input(s): Nest Size (NS) & Terminating condition (tc)
Output(s): Fittest Key bits
Set t← 0   {/*Initialization Parameter */}
FOR i= 0 to (NS-1) do
    Produce initial population of key bits (host)
    Evaluate the fitness function for each key bit (host egg) f($x_i^{t}$).f($x_i^t$)
END FOR
DO
    Generate a new key bits (CS) :levy flight(random number) f($x_i^{t+1}$).
    Select a nest out of NS solutions on random basis.
    IF [$f(xi\,t+1) < f(xi\,t)$] THEN
        Replace it with the solution f($x_i^{t}$).
    END IF
    Discard the worse case nest.
    Develop a new nest at new position by Levy flight.
    Keep the best solution and evaluate the next current best solution.
    $Increment\ t$
UNTIL ( $t <= tc$ )
```

```
    Generate the best key bits.
```

By the help of pre-defined mask generation algorithm [6-8], a mask matrix of order [n] by [$^{n}C_{k-1}$], where n in the number of fragments an k is the number of threshold fragments. The following algorithm explains the fragmentation concept. The source file would be broken into homogeneous blocks of static length. If needed padding of zeros may be done in case of the last block to make homogeneous blocks.

Algorithm 3: Proposed Fragmentation (MS[n][$^{n}C_{k-1}$], SF[ ][ ])

Input(s): Masked Matrix & Source File

Output(s): n number of fragmented files

```
Set S← ( SizeOf( SF[ ][ ]) DIV $^{n}C_{k-1}$ )
Set R← ( SizeOf( SF[ ][ ]) MOD $^{n}C_{k-1}$)
if( R != 0 ) then
  SF[ ][ ]←Call AppendBit(SF[ ][ ],($^{n}C_{k-1}$*S ), ($^{n}C_{k-1}$-R), 0)
else
for i = 1 to n do
    while ( !EOF (SF[ ][ ]) do
            FFILE[i][ $^{n}C_{k-1}$ ] ← Call SubsequentXOR(MS[i][ $^{n}C_{k-1}$ ] , SF[$^{n}C_{k-1}$ ])
     end while
end for
end if
```

Using the above stated algorithm, the n number of encrypted key fragments and file fragments are obtained. The next algorithm will discuss about the second round of encryption. N number of different blocks will be created by XORing the key fragments followed by its file fragments of same order. N/2 number of separate blocks to be created depending upon the following Check_Fragstatus(integer) followed by XORing.

Mathematically, the formula for even number is $(2 * n)$ and for odd number $(2 * n + 1)$, where n is any integer.

Now we will check which key fragment and file fragment is even or odd from fragment matrix using following function Check_Fragstatus (integer). Pseudo code of function is as follows.

```
Check_Fragstatus(int fragnum)
{
  if (fragnum mod 2=0) then
          return "even fragment"
  return "odd fragment"
  end if
}
```

Algorithm 4: Proposed Block_Fusion (FKEY[n][$^{n}C_{k-1}$], FFILE[n][$^{n}C_{k-1}$])

Input(s): Array: FKEY[n][$^{n}C_{k-1}$] & FFILE[n][$^{n}C_{k-1}$]

Output(s): Product ciphered matrix

```
for i = 1 to n do
     Blocks[i] [ $^{n}C_{k-1}$ ] ← Call SubsequentXOR (FFILE[i][ $^{n}C_{k-1}$ ], FKEY[i][ $^{n}C_{k-1}$ ])
 end loop
for i = 1 to n do
   temp ← Call Check_Fragstaus ( i )
    if ( temp ) then
        EvenBlocks[n/2] [ $^{n}C_{k-1}$ ] ← Call SubsequentXOR ( Blocks[i] [ $^{n}C_{k-1}$ ]
     else
        OddBlocks[n/2] [ $^{n}C_{k-1}$ ] ← Call SubsequentXOR ( Blocks[i] [ $^{n}C_{k-1}$ ]
     end if
end loop
 TFILE[n]← Call SubsequentXOR(EvenBlocks[n/2] [ $^{n}C_{k-1}$ ], OddBlocks[n/2] [ $^{n}C_{k-1}$ ] )
Ready transmittable file
```

VI. RESULTS AND DISCUSSION

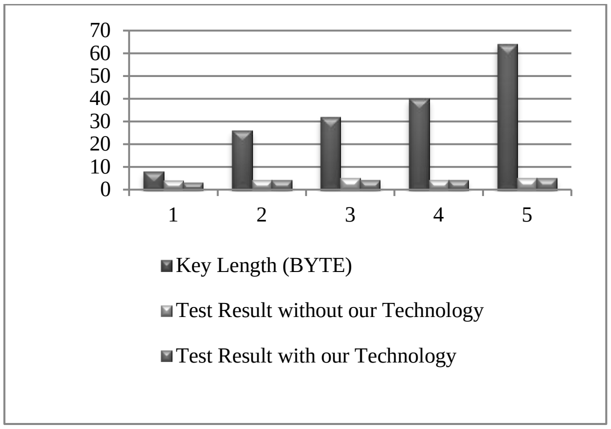
In the result section we use a statistical randomness test such as serial test which proves the randomness of our key. The following table of tests results shows that the randomness of key is at per level of standard algorithm Triple DES [7] in average. For small (16 to 40 bytes) key size our technique shows better result but for large key size our technique is showing at per level of results.

Table 1 : Data Value from Serial Test

Key size (byte)	Test result on key by prng( )	Test result of this technique
08	4.0214	3.0636
16	4.1128	4.0973
32	5.1965	4.1843
40	4.2043	4.1992
64	4.1077	5.0000

From table 1, it can be stated that for the key length eight bytes, the proposed technique has yielded 3.0636 with respect to 4.0214 for random generating functions. Doubling the key length, the proposed technique has given almost equivalent results with 4.0973 value. For thiry two bytes key size, it has been observed that it gives better results as 4.1843 compared to 5.1965 value. More or less at par results obtained in case of forty bytes key length.

Figure 1: Bar Graph Analysis on Table 1.

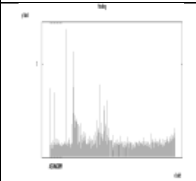
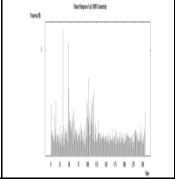
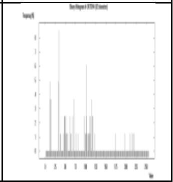


The above mentioned graph analysis also proves our experiment and observations.

ANALYSIS OF HISTOGRAM

The histogram comparison has been given in the following figure 2. Parallel comparison between the histogram of the normal text, triple DES, and proposed ciphered technique is done.

Figur 2 :Comparison on basis of Histogram

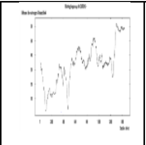
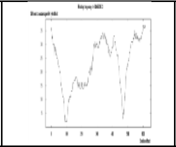
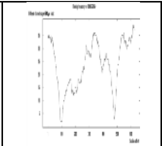
TOOL	**NORMAL TEXT**	**TRIPLE DATA ENCRYPTION STANDARD**	**PROPOSED CIPHERED TECHNIQUE**
Histogram			

The histogram generated from the cipher text of the proposed technique shows better distribution patterns with respect to normal text and triple DES.

ANALYSIS OF FLOATING POINT FREQUENCY

The comparison in terms of floating point frequency has been shown in the following figure 3.

Figur 3 :Comparison on basis of Floating Point Frequency

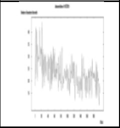
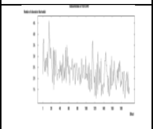
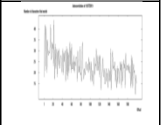
TOOLS	**NORMAL TEXT**	**TRIPLE DATA ENCRYPTION STANDARD**	**PROPOSED CIPHERED TECHNIQUE**
FP Frequency			

From figure 3, the floating point frequency graph generated by the proposed technique is at par with respect to triple DES encryption method and better than normal text.

ANALYSIS OF AUTO CORELATION

Figure 4 representing the auto corelation graph for the comparative study between the proposed technique, normal text, and triple DES.

Figur 4 :Comparison on basis of Auto corelation

TOOLS	**NORMAL TEXT**	**TRIPLE DATA ENCRYPTION STANDARD**	**PROPOSED CIPHERED TECHNIQUE**
Autocorelation			

Observation from figure 4, the auto correlation graph obtained from the proposed technique is more or less equivalent to the triple DES encryption method and much robust than normal text.

VII. CONCLUSION AND FUTURE SCOPE

The proposed methodology of encryption shows favourable outcomes in terms of different randomness test. Here optimization technique such as cuckoo search algorithm, file and data fragment concept provides uniqueness of our scheme. The robustness of our key is proved by different statistical tests and this provides a strong encryption.

In future this scheme can be used in expert systems, and in broad sense of medical domain.

REFERENCES

[1]. Mandal, B. K., Bhattacharyya, D., & Bandyopadhyay, S. K., Designing and Performance Analysis of a Proposed Symmetric Cryptography Algorithm, In the Proceedings of the International Conference on Communication Systems and Network Technologies
(CSNT 2013), April 6-8 2013, Gwalior, India, pp. 453-461.

[2]. Christian Blum, Ant Colony Optimization: Introduction and recent trends,Physics of Life Review, Elsevier, Vol. 2, Issue 4, December 2005, pp. 353-373

[3]. Ping Duan, Yong AI, Research on an Improved Ant Colony

Optimization Algorithm and its application, International Journal of
Hybrid Information Technology Vol.9, No.4 (2016), pp. 223-234.

[4]. Clark, J.A., Nature-Inspired Cryptography: Past, Present and Future, In Proceedings of Conference on Evolutionary Computation,
December 8-12, 2003, Canberra, Australia.

[5]. M. Mareli, B. Twala, An adaptive cuckoo search algorithm for optimisation, Applied Computing and Informatics, Volume 14, Issue 2, pp. 107-115, July. 2018.

[6]. 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

[7]. Preeti Singh et al, "Symmetric Key Cryptography: Current Trends", International Journal of Computer Science and Mobile Computing,
Vol.3 Issue.12, December- 2014, pg. 410-415.

[8]. H. F. Hua ng and C.C. Chang "A novel efficient (t, n) threshold proxy signature scheme", Information Sciences 176(10): 1338-1349, 2006.

[9]. Bozkurt, Kaya, Selcuk, Guloglu ,"Threshold Cryptography Based On Blakely Secret Sharing", Information Sciences 177(19):4148–4160, 2008.

[10]. Stallings William, "Cryptography and Network Security", Pearson India Education Service Pvt. Ltd., pp.111-155, 2015

Authors Profile

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. He is working as Leturer in Department of Computer Sciences at M.U.C. Women's College, Burdwan West Bengal, India since 2011. He has published two conferences papers and it's also available online. His main research work focuses on Cryptography and Computational Intelligence.. He has 7.5 years and 0.5 years of teaching experience at UG and PG level respectively.

.

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. His research interests include Network Security, E-Commerce, and Bioinformatics. He has published numerous papers in both national as well as international journals and conferences.

Dr. ARINDAM SARKAR is currently serving the Deparment of Computer Science & Electronics, amakrishna 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 Rand in the West Bengal College Service Commission examination. He has more than 50 International Journal and Conference publications.

Anirban Bhowmik completed Bachelor of Science (Mathematics) 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 Application at Cyber Research & Training Institute, Burdwan ,West Bengal, India since 2008. He has published two conferences papers and it's also available online. His main research work focuses on Cryptography and Soft Computing. He has 10 years of teaching experience at UG level.