International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 2 Issue 10, October - 2013

New Cryptography Method Using Relative Displacement: RDC Symmetric Key Algorithm

Nehal Kandele, Shrikant Tiwari
Department of Computer Science & Engineering (CSE)
Shri Shankaracharya Technical Campus (SSTC), Shri Shankaracharya Group of Institutions (SSGI)
Faculty of Engineering and Technology, Junwani, Bhilai, District-Durg, C.G., 490020

Abstract

The author proposes a new symmetric key encryption algorithm which is based on the following steps: 1) In the first step, converting each character of the string into its corresponding ASCII value and dividing the string into square matrices of maximum possible even order. 2) In the second step, calculating the key1 and key2 and thereby deducing key on the basis of these keys. 3) In the third step, performing a sequence of row interchange operation, followed by a sequence of rotation operation on each derived square matrix. 4) In the fourth step, adding magic square matrix of same size as that of the matrix under consideration. 5) In the fifth and final step, the remaining elements are modified by adding to them, the product of sum of the magic square of size same as that of the derived key and the successor of the corresponding position of each element in the series of remaining elements.

1. Introduction

All the cryptographic algorithm aim to convert the plain text; that is input string, into a cipher text, the encrypted message, which is as difficult as possible to decode and understand. The decoding becomes further complicated if the key is abstracted or not used. A good cryptographic algorithm is a technique that cannot be easily traced and the only method to trace it is the hit and trial method for all possible and available techniques. Encryption algorithms may be symmetric or asymmetric.

In symmetric encryption, the process of encryption and decryption is performed with the help of a common key, which should be either known or should be transmitted to both, the sender and the receiver, before the encryption and decryption takes place.

In asymmetric key, the problem of key transmission is resolved. It employs the use of two types of keys, private key and public key. Private Key or secret key is called so, since it is unknown to others. Public key is used for the encryption of data whereas private key is used for decryption. In the present work, the string is fragmented into square matrix of even order and then rotation pattern is designed in such a way that, every element is not only displaced from its original position but also the adjacent neighbours of the elements are changed. A magic square matrix of size, same as that of resultant matrix is then added to it, to change the number of occurrence of the characters. The elements which could not be accommodated in the matrix are also modified in the similar way.

2. Basic terminology

Magic square matrix

Magic square matrix is a square matrix in which the sum of all elements in each column and in each row is same. The sum can be calculated from the formula $(n*(n^2+1))/2$, where n is the size of square matrix.

Pattern rotation

Pattern rotation involves a series of steps to shift the position of elements in a particular predefined pattern.

A square matrix of even order

A square matrix of even order refers to a matrix with equal number of rows and columns and this number is even, that is divisible by 2. Example, matrix of order 2x2, 4x4, 6x6, etc.

3. Proposed encryption algorithm

Step-1

We calculate the length of the given input string and assign it to variable N. Each element of the input string is then converted into its corresponding ASCII value.

Consider that the entered input string is "SUN RISES IN THE EAST!"
Here, length of string N = 22, so the ASCII equivalent of the string is:
[83 85 78 32 82 73 83 69 83 32 73 78 32 84 72 69 32 69 65 83 84 33]

Step-2

We break the input string into square matrices of maximum possible size of even order and place the remaining elements into a variable REM. This step is repeated, using remainder REM of this step as input string, until there are 4 or more elements in REM.

So, in this example matrices are:

$$\begin{bmatrix} 83 & 85 & 78 & 32 \\ 82 & 73 & 83 & 69 \\ 83 & 32 & 73 & 78 \\ 32 & 84 & 72 & 69 \end{bmatrix}_{4\times4} \begin{bmatrix} 32 & 69 \\ 65 & 83 \end{bmatrix}_{2\times2} \text{REM= [84 33]}$$

Step-3

Calculating the KEY by KEY1 ⊛ KEY2, where, KEY1 can be calculated as sum of numbers of columns of all matrices and number of elements in REM. KEY2 can be calculated as the sum of magic square matrix of size same as that of last generated square matrix. Here, ⊛ refers to addition. If the KEY is greater than 9, then sum all the digits until a single digit KEY is obtained.

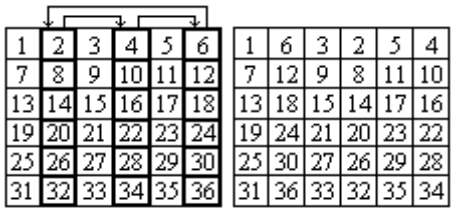
Here, KEY1 = 4 + 2 + 2 = 8, Size of last generated square matrix = 2 and sum of magic square matrix of size 2 = 5
So, KEY2 = 5, and KEY = 8 ⊛ 5 = 13 = 1 + 3 = 4

Step-4

In this step, we apply a rotation pattern on the square matrices obtained. The sequence of the steps in rotation pattern can be listed as follows, assume that the matrix is:

1	2	3	4	5	6
7	8	9	10	11	12
13	14	15	16	17	18
19	20	21	22	23	24
25	26	27	28	29	30
31	32	33	34	35	36

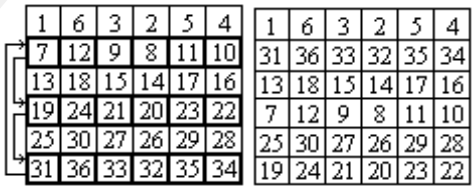
(i) In the first rotation interchanging the even columns in the following manner:



1	2	3	4	5	6
7	8	9	10	11	12
13	14	15	16	17	18
19	20	21	22	23	24
25	26	27	28	29	30
31	32	33	34	35	36

1	6	3	2	5	4
7	12	9	8	11	10
13	18	15	14	17	16
19	24	21	20	23	22
25	30	27	26	29	28
31	36	33	32	35	34

(ii) In second rotation interchanging the even rows in the following manner:



1	6	3	2	5	4
7	12	9	8	11	10
13	18	15	14	17	16
19	24	21	20	23	22
25	30	27	26	29	28
31	36	33	32	35	34

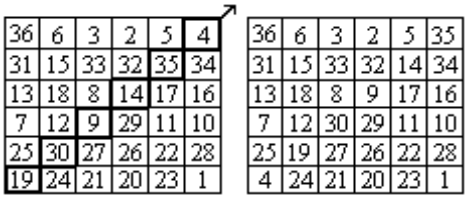
1	6	3	2	5	4
31	36	33	32	35	34
13	18	15	14	17	16
7	12	9	8	11	10
25	30	27	26	29	28
19	24	21	20	23	22

(iii) In third rotation performing single-diagonal-left-up shift as shown below:

1	6	3	2	5	4
31	36	33	32	35	34
13	18	15	14	17	16
7	12	9	8	11	10
25	30	27	26	29	28
19	24	21	20	23	22

36	6	3	2	5	4
31	15	33	32	35	34
13	18	8	14	17	16
7	12	9	29	11	10
25	30	27	26	22	28
19	24	21	20	23	1

(iv) In fourth rotation performing single-diagonal-right-up shift as shown below:



36	6	3	2	5	4
31	15	33	32	35	34
13	18	8	14	17	16
7	12	9	29	11	10
25	30	27	26	22	28
19	24	21	20	23	1

36	6	3	2	5	35
31	15	33	32	14	34
13	18	8	9	17	16
7	12	30	29	11	10
25	19	27	26	22	28
4	24	21	20	23	1

(v) In fifth rotation applying single-up shift to the every even column as follows:

36	6	3	2	5	35
31	15	33	32	14	34
13	18	8	9	17	16
7	12	30	29	11	10
25	19	27	26	22	28
4	24	21	20	23	1

36	15	3	32	5	34
31	18	33	9	14	16
13	12	8	29	17	10
7	19	30	26	11	28
25	24	27	20	22	1
4	6	21	2	23	35

(vi) In the sixth and last rotation rotating once the outer most cycle in clock wise direction, its inner circle in anti-clock wise direction, and so on as shown below:

36→	15→	3→	32→	5→	34↓
↑31	18↓	←33	←9	←14	16↓
↑13	12↓	8→	29↓	↑17	10↓
↑7	19↓	↑30	←26	↑11	28↓
↑25	24→	27→	20→	↑22	1↓
↑4	←6	←21	←2	←23	←35

31	36	15	3	32	5
13	33	9	14	17	34
7	18	30	8	11	16
25	12	26	29	22	10
4	19	24	27	20	28
6	21	2	23	35	1

So, the resultant matrices of above example after these rotation operations are:

$$\begin{bmatrix} 32 & 69 & 73 & 78 \\ 83 & 78 & 73 & 84 \\ 85 & 82 & 69 & 32 \\ 32 & 83 & 72 & 83 \end{bmatrix} \begin{bmatrix} 69 & 83 \\ 65 & 32 \end{bmatrix}$$

Step-5

A magic square matrix of same size as that of the square matrix, under the consideration, is then added to it.

$$\begin{bmatrix} 32 & 69 & 73 & 78 \\ 83 & 78 & 73 & 84 \\ 85 & 82 & 69 & 32 \\ 32 & 83 & 72 & 83 \end{bmatrix} + \begin{bmatrix} 16 & 2 & 3 & 13 \\ 5 & 11 & 10 & 8 \\ 9 & 7 & 6 & 12 \\ 4 & 14 & 15 & 1 \end{bmatrix} = \begin{bmatrix} 48 & 71 & 76 & 91 \\ 88 & 89 & 83 & 92 \\ 94 & 89 & 75 & 44 \\ 36 & 97 & 87 & 84 \end{bmatrix}$$

$$\begin{bmatrix} 69 & 83 \\ 65 & 32 \end{bmatrix} + \begin{bmatrix} 1 & 3 \\ 4 & 2 \end{bmatrix} = \begin{bmatrix} 70 & 86 \\ 69 & 34 \end{bmatrix}$$

Step-6

Now we calculate the variable F as the sum of magic square matrix of order KEY. Adding F * (n + 1) to each n^{th} term in the REM, to generate final REM.

Here, REM= [84 33], KEY = 4, sum of magic square matrix of order 4 = 34, therefore F = 34,
Final REM = [84 + (34 * (1 + 1)) 33 + (34 * (2 + 1))]
= [152 135]

Step-7

In the last step, we merge all the square matrices and the remainder, in the order they were derived, and then convert these ASCII values into characters to form the cipher text.

$$\begin{bmatrix} 48 & 71 & 76 & 91 \\ 88 & 89 & 83 & 92 \\ 94 & 89 & 75 & 44 \\ 36 & 97 & 87 & 84 \end{bmatrix} \begin{bmatrix} 70 & 86 \\ 69 & 34 \end{bmatrix} [152\ 135]$$

String = [48 71 76 91 88 89 83 92 94 89 75 44 36 97 87 84 70 86 69 34 152 135]
So, cipher text is:
0GL[XYS\^YK,$aWTFVE”Öç

4. Proposed decryption algorithm

Step-1

We calculate the length of the given input string and assign it to variable N. Each element of the input string is then converted into its corresponding ASCII value.

Consider that the entered input string is:
“ 0GL[XYS\^YK,$aWTFVE”Öç”
Here, length of string N = 22
So, the ASCII equivalent of the string is [48 71 76 91 88 89 83 92 94 89 75 44 36 97 87 84 70 86 69 34 152 135]

Step-2

We break the input string into square matrices of maximum possible size of even order and place the remaining elements into a variable REM. This step is repeated, using remainder REM of this step as input string, until there are 4 or more elements in REM.

So, in this example matrices are:

$$\begin{bmatrix} 48 & 71 & 76 & 91 \\ 88 & 89 & 83 & 92 \\ 94 & 89 & 75 & 44 \\ 36 & 97 & 87 & 84 \end{bmatrix}_{4\,x\,4} \begin{bmatrix} 70 & 86 \\ 69 & 34 \end{bmatrix}_{2\,x\,2} \text{REM= [152 135]}$$

Step-3

Calculating the KEY by KEY1 ⊛ KEY2, where, KEY1 can be calculated as sum of numbers of columns of all matrices and number of elements in REM. KEY2 can be calculated as the sum of magic square matrix of size same as that of last generated square matrix. Here, ⊛ refers to addition. If the KEY is greater than 9, then sum all the digits until a single digit KEY is obtained.

Here KEY1 = 4 + 2 + 2 = 8,
Size of last generated square matrix=2 and sum of magic square matrix of size 2=5
So, KEY2 = 5 and KEY = 8 ⊛ 5 = 13 = 1 + 3 = 4

Step-4

A magic square matrix of same size as that of the square matrix, under the consideration, is then subtracted to it.

$$\begin{bmatrix} 48 & 71 & 76 & 91 \\ 88 & 89 & 83 & 92 \\ 94 & 89 & 75 & 44 \\ 36 & 97 & 87 & 84 \end{bmatrix} - \begin{bmatrix} 16 & 2 & 3 & 13 \\ 5 & 11 & 10 & 8 \\ 9 & 7 & 6 & 12 \\ 4 & 14 & 15 & 1 \end{bmatrix} = \begin{bmatrix} 32 & 69 & 73 & 78 \\ 83 & 78 & 73 & 84 \\ 85 & 82 & 69 & 32 \\ 32 & 83 & 72 & 83 \end{bmatrix}$$

$$\begin{bmatrix} 70 & 86 \\ 69 & 34 \end{bmatrix} - \begin{bmatrix} 1 & 3 \\ 4 & 2 \end{bmatrix} = \begin{bmatrix} 69 & 83 \\ 65 & 32 \end{bmatrix}$$

Step-5

In this step, we apply a rotation pattern on the square matrices obtained. The sequence of the steps in rotation pattern can be listed as follows, assume that the matrix is:

1	2	3	4	5	6
7	8	9	10	11	12
13	14	15	16	17	18
19	20	21	22	23	24
25	26	27	28	29	30
31	32	33	34	35	36

(i) In the first rotation rotating once the outer most cycle in anti clock wise direction, its inner circle in clock wise direction, and so on as shown below:

1 ↓	←2	←3	←4	←5	←6
7 ↓	8→	9→	10→	11 ↓	↑ 12
13 ↓	↑ 14	15 ↓	←16	17 ↓	↑ 18
19 ↓	↑ 20	21→	↑ 22	23 ↓	↑ 24
25 ↓	↑ 26	←27	←28	←29	↑ 30
31→	32→	33→	34→	35→	↑ 36

2	3	4	5	6	12
1	14	8	9	10	18
7	20	16	22	11	24
13	26	15	21	17	30
19	27	28	29	23	36
25	31	32	33	34	35

(ii) In second rotation applying single-down shift to the every even column as follows:

2	3	4	5	6	12
1	14	8	9	10	18
7	20	16	22	11	24
13	26	15	21	17	30
19	27	28	29	23	36
25	31	32	33	34	35

2	31	4	33	6	35
1	3	8	5	10	12
7	14	16	9	11	18
13	20	15	22	17	24
19	26	28	21	23	30
25	27	32	29	34	36

(iii) In third rotation performing single-diagonal-left-down shift as shown below:

2	31	4	33	6	35
1	3	8	5	10	12
7	14	16	9	11	18
13	20	15	22	17	24
19	26	28	21	23	30
25	27	32	29	34	36

2	31	4	33	6	25
1	3	8	5	35	12
7	14	16	10	11	18
13	20	9	22	17	24
19	15	28	21	23	30
26	27	32	29	34	36

(iv) In fourth rotation performing single-diagonal-right-down shift as shown below:

2	31	4	33	6	25
1	3	8	5	35	12
7	14	16	10	11	18
13	20	9	22	17	24
19	15	28	21	23	30
26	27	32	29	34	36

36	31	4	33	6	25
1	2	8	5	35	12
7	14	3	10	11	18
13	20	9	16	17	24
19	15	28	21	22	30
26	27	32	29	34	23

(v) In fifth rotation interchanging the even rows in the following manner:

36	31	4	33	6	25
1	2	8	5	35	12
7	14	3	10	11	18
13	20	9	16	17	24
19	15	28	21	22	30
26	27	32	29	34	23

36	31	4	33	6	25
13	20	9	16	17	24
7	14	3	10	11	18
26	27	32	29	34	23
19	15	28	21	22	30
1	2	8	5	35	12

(vi) In the sixth and last rotation interchanging the even columns in the following manner:

36	31	4	33	6	25
13	20	9	16	17	24
7	14	3	10	11	18
26	27	32	29	34	23
19	15	28	21	22	30
1	2	8	5	35	12

36	33	4	25	6	31
13	16	9	24	17	20
7	10	3	18	11	14
26	29	32	23	34	27
19	21	28	30	22	15
1	5	8	12	35	2

So, resultant matrices of above example after these rotation operations are:

$$\begin{bmatrix} 83 & 85 & 78 & 32 \\ 82 & 73 & 83 & 69 \\ 83 & 32 & 73 & 78 \\ 32 & 84 & 72 & 69 \end{bmatrix} \begin{bmatrix} 32 & 69 \\ 65 & 83 \end{bmatrix}$$

Step-6

Now we calculate the variable F as the sum of magic square matrix of order KEY. Subtracting F * (n + 1) from each n^{th} term in the REM, to generate final REM.

Here, KEY = 4, REM= [152 135], sum of magic square matrix of order 4 = 34, therefore, F = 34
Final REM = [152 - (34 * (1 + 1)) 135 - (34 * (2 + 1))]
= [84 33]

Step-7

In the last step, we merge all the square matrices and the remainder, in the order they were derived, and then convert these ASCII values into characters to form the plain text.

Here, matrices are:

$$\begin{bmatrix} 83 & 85 & 78 & 32 \\ 82 & 73 & 83 & 69 \\ 83 & 32 & 73 & 78 \\ 32 & 84 & 72 & 69 \end{bmatrix} \begin{bmatrix} 32 & 69 \\ 65 & 83 \end{bmatrix} [84\ 33]$$

String = [83 85 78 32 82 73 83 69 83 32 73 78 32 84 72 69 32 69 65 83 84 33]
So, plain text is:

SUN RISES IN THE EAST!

5. Result

Following String-Time graph displays the time taken for the encryption of varying string length. The corresponding Character-Time graph showing the average time taken to encrypt each character for the varying length of string is given below.

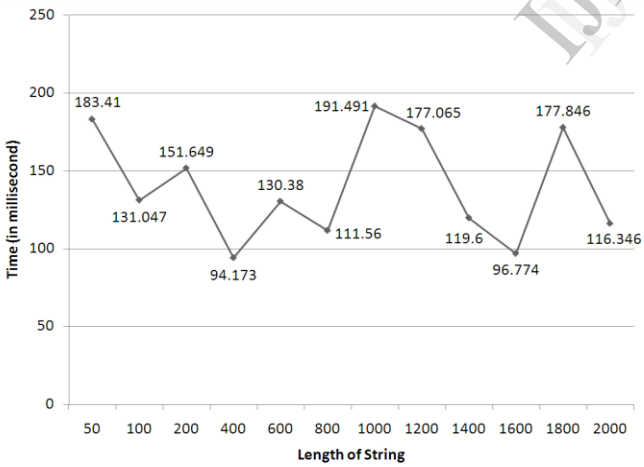


Figure 1. Sting-Time graph

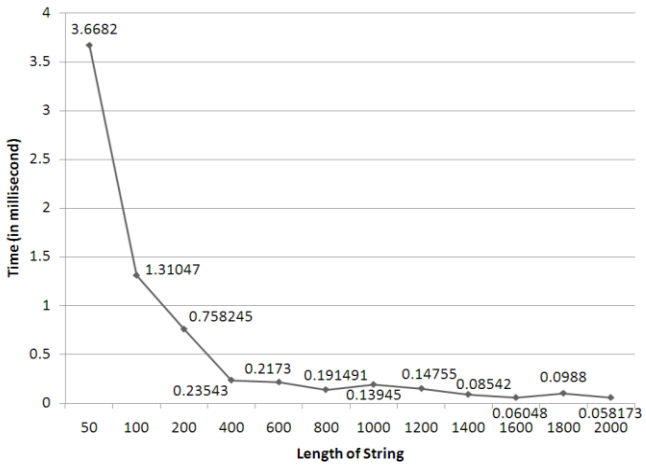


Figure 2. Character-Time graph

6. Conclusion

In the present work, we use keyless keying, that is keying or encrypting the data without using a predefined or a fixed key. Also, the requirement of key transmission is removed. The key changes with increase in length of string without increasing the complexity. So, in this algorithm, it is nearly impossible to decrypt the encrypted text without knowing the criteria to generate key. The rotation pattern is designed to conceal the recognition of pattern in the string.

7. Acknowledgement

I am highly indebted to Dr. R. N. Patel sir for his invaluable guidance and suggestions. I owe much of thanks to my brother, Suyash Kandele for his support.

8. References

[1] Ya-Ping Zhang, Jizhou Sun, and Xu Zhang, "A Stream Cipher Algorithm Based on Conventional Encryption Techniques", *IEEE*, 0-7803-8253-6/04, 2004.
[2] A. Chandra Sekhar, K.R. Sudha, and Prasad Reddy P V G D, "Data Encryption technique using Random number generator", *IEEE Computer Society*, 0-7695-3032-X/07, DOI 10.1109/GrC.2007.73, 2007.
[3] Albert H. Carlson, Robert E. Hiromoto, and Richard B. Wells, "Breaking Block and Product Ciphers Applied Across Byte Boundaries", *IEEE*, 978-1-4577-1425-2/11, 2011
[4] Dripto Chatterjee, Suvadeep Dasgupta, Joyshree Nath, and Asoke Nath, "A new Symmetric key Cryptography Algorithm using extended MSA method: DJSA symmetric key algorithm", *IEEE*, 978-0-7695-4437-3/11, DOI 10.1109/CSNT.2011.25, 2011.
[5] Zhang Yunpeng, Zhu Yu, Wang Zhong, and Richard O.Sinnott, "Index-Based Symmetric DNA Encryption Algorithm", *IEEE*, 978-1-4244-9306-7/11, 2011.
[6] Neeraj Khanna, Joyshree Nath, Joel James, Amlan Chakrabarti, Sayantan Chakraborty, and Asoke Nath, "New Symmetric Key Cryptographic algorithm using combined bit manipulation and MSA encryption algorithm: NJJSAA symmetric key algorithm", *IEEE Computer Society*, 978-0-7695-4437-3/11, DOI 10.1109/ CSNT.2011.33, 2011.
[7] D. Rajavel, and S. P. Shantharajah, "Cubical Key Generation and Encryption Algorithm Based on Hybrid Cube's Rotation", *IEEE*, 978-1-4673-1039-0/12, March 21-23, 2012.
[8] Marcin Niemiec, and Lukasz Machowski, "A new symmetric block cipher based on key-dependent S-boxes", *IEEE*, 978-1-4673-2015-3/12, 2012.
[9] Hai Cheng, and Qun Ding "Overview of the Block Cipher", *IEEE Computer Society*, 978-0-7695-4935-4/12, DOI 10.1109/IMCCC.2012.379, 2012.
[10] Gaurav Bhadra, Tanya Bala, Samik Banik, Asoke Nath, and Joyshree Nath,"Bit Level Encryption Standard (BLES): Version-II", *IEEE*, 978-1-4673-4805-8/12, 2012.
[11] Rishav Ray, Jeeyan Sanyal, Debanjan Das, and Asoke Nath, "A new Challenge of hiding any encrypted secret message inside any Text/ASCII file or in MS word file: RJDA Algorithm", *IEEE*, 978-0-7695-4692-6/12, DOI 10.1109/CSNT.2012.191, 2012.
[12] Somdip Dey, "SD-C1BBR: SD-Count-1-Byte-Bit Randomization: A New Advanced Cryptographic Randomization Technique", *IEEE*, 978-1-4673-4805-8/12, 2012.
[13] Akanksha Mathur, "A Research paper: An ASCII value based data encryption algorithm and its comparison with other symmetric data encryption algorithms", *International Journal on Computer Science and Engineering*, ISSN: 0975-3397, vol. 4, no. 09, 2012, pp. 1650-1657.
[14] Sayak Guha, Tamodeep Das, Saima Ghosh, Joyshree Nath, Sankar Das, and Asoke Nath, "A New Data Hiding Algorithm With Encrypted Secret Message Using TTJSA Symmetric Key Crypto System", *Journal of Global Research in Computer Science*,ISSN-2229-371X, vol. 3, no. 4, April 2012.
[15] Somdip Dey, "SD-AREE: An Advanced Modified Caesar Cipher Method to Exclude Repetition from a Message", *International Journal of Information and Network Security*, vol. 1, no. 2, ISSN: 2089-3299, June 2012.
[16] Rajavel D, and Shantharajah S. P, "Cryptography Based on Combination of Hybridization and Cube's Rotation", *International Journal of Computational Intelligence and Informatics*, vol. 1: no. 4, ISSN: 2231-0258, March 2012.
[17] Somdip Dey, Joyshree Nath, and Asoke Nath, "An Integrated Symmetric Key Cryptographic Method-Amalgamation of TTJSA Algorithm, Advanced Caesar Cipher Algorithm, Bit Rotation and Reversal Method: SJA Algorithm", *I. J. Modern Education and Computer Science*, DOI: 10.5815/ijmecs.2012.05.01, 2012.
[18] Somdip Dey, Kalyan Mondal, Joyshree Nath, and Asoke Nath, "Advanced Steganography Algorithm Using Randomized Intermediate QR Host Embedded With Any Encrypts Secret Message: ASA_QR Algorithm", *I. J. Modern Education and Computer Science*, DOI: 10.5815/ijmecs.2012.06.08, 2012.
[19] Mr. Rangaswamy D. A., and Mr. Punithkumar M. B., "New Symmetric Key Cryptographic Algorithm Using Combined Bit Manipulation and MSA Encryption Algorithm: NJJSAA Symmetric Key Algorithm", *International Journal of Innovative Research and Development*, vol. 2, Issue 6, ISSN: 2278-0211, June 2013.
[20] Thanapal P, Muthamil Selvan T, and Pratheeba T, "An Integrated Cryptography Approach Using MSA Symmetric Key", *International Journal of Engineering Research and Technology*, vol. 2, Issue 3, ISSN:2278-0181, March 2013

Nehal Kandele, B.E., M.E. Scholar in Computer Technology & Application from Shri Shankaracharya Technical Campus, Bhilai, Chhattisgarh, India. Research areas are Computer Network and Cryptography.

Dr. Shrikant Tiwari, currently working as Assistant Professor in Department of Computer Science & Engineering at Shri Shankaracharya Technical Campus, Bhilai, Chhattisgarh, India. He has received his Ph.D in Department of Computer Science and Engineering from the Indian Institute of Technology (Banaras Hindu University), Varanasi. He has published more than 20 papers in international journal and conference and also published 5 Book Chapters.