**International Journal of Data Informatics and Intelligent computing (IJDIIC)**
Vol. 2, No. 1, March 2023, pp. 42~50
DOI: 10.59461/ijdiic.v2i1.38

# Cryptographic Interweaving of Messages

**Jagadeesh Sai D[1], Krishnaraj P M[1]**
[1]Department of Information Science and Engineering, Ramaiah Institute of Technology, Bengaluru, Visveswaraya Technological University, India

**Article Info**

***Article history:***

Received February 11, 2023
Revised March 02, 2023
Accepted March 18, 2023

***Keywords:***

Cryptography
Encryption
Ciphertext
Session key
Matrix traversal

**ABSTRACT**

During the past several decades, the information and communication technology sector has advanced significantly, enabling extensive information interchange over the internet, including message sharing and electronic transactions. These days, the main issue is how to transmit information securely. From ancient times, there has been interest in the field of cryptography research. A masterwork of cryptography is Muni Kumudendu's original work, Siribhoovalaya. His study served as the basis for the method suggested in this publication. Several messages can be sent using different keys utilising a single matrix. Encryption uses a variety of matrix traversal techniques, making it challenging for cryptanalysis to map the plaintext and ciphertext.



***Corresponding Author:***

Jagadeesh sai D
Depatment of Information Science and Engineering
Ramaiah Institute of Technology
Bengaluru
India
Email: djsai@msrit.edu

## 1. INTRODUCTION

Cryptography is the process of sending and receiving the messages securely over any communication medium. It involves Encryption, the process of transferring the plaintext to a ciphertext and Decryption, the process of converting the ciphertext back to the plaintext. [1][2]Besides the plaintext and ciphertext, a key is used which determines functional output of the cryptographic algorithm. Symmetric key encryption uses the same key for encryption as well as decryption. The key is exchanged securely using any key exchanging algorithm. Asymmetric key encryption uses different keys for encryption and decryption with some mathematical relation between them[3][4].

Various research work is been carried out in the area of cryptography. The paper [5] describes about Siri Bhoovalaya, which is one of the intriguing pieces of literature created by Muni Kumudendu thousands of years ago. It contains the scripts written in numerals only which can be deciphered as the poetry and verses in Kannada, Hindi, Sanskrit and other different languages. The script consists of the numerals from 1 to 64 arranged in 27x27 matrix. A mono substitution table is used to map these numbers to phonetic alphabets.
Each matrix (27x27) is known as 'Chakra'. The Chakra consists of the encrypted verses. 'Bandha' is used to decipher the Chakra which can be another matrix, symbol or any other ways to traverse the original matrix. Similar concept we have used in our algorithm also. Based on the key matrix, the ciphertext matrix is traversed to get the original message.

In Chakra-Bandha scheme the whole 27x27 matrix is arranged in different orientation and another same size matrix is used to decipher it. In Namak-Bandhas, each Chakra is divided into smaller 9x9 matrices and transposition scheme is applied on those. Also, different Steganographic schemes are used in which

various symbols are used for traversing the matrix. In this way, substitution, transposition and steganographic schemes are used in this script making it interesting area of research with reference to the paper [6].

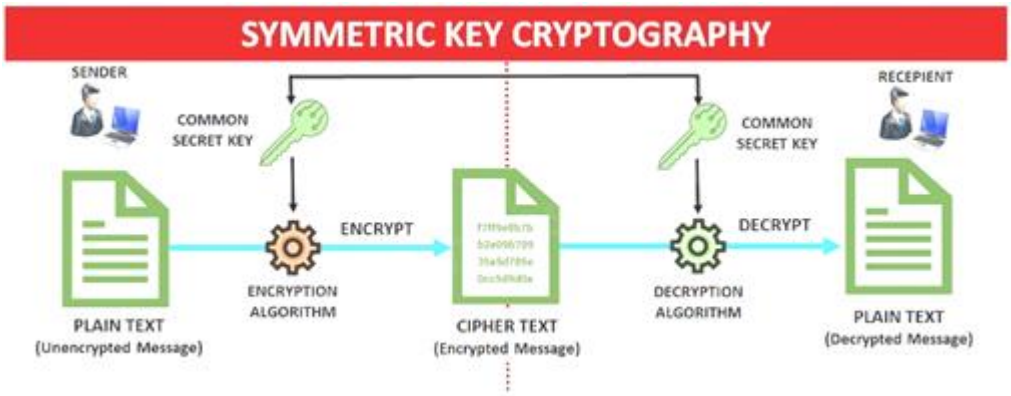


Figure 1. Architecure of Cryptographic Interweaving

In Figure 1 the key is converted into its ascii equivalent, and a set of random numbers is sent to the receiver as well. These random numbers are added to get the nearest possible palindrome number which is used to manipulate the original matrix to produce a cipher matrix which is then multiplied with the original matrix to get an encoded matrix which is fit for transmission. The decryption of data involves calculating inverse of the cipher matrix and its multiplication with the encoded matrix and the resulting matrix is manipulated using the palindrome number generated via key and random numbers that were obtained to get the original data matrix[7].

## 2. RELATED WORK

the Vigenère cipher and the Playfair cipher.The Vigenère cipher is a method of encrypting alphabetic text. It uses a simple form of polyalphabetic substitution, where a letter in the plaintext is shifted by a certain number of positions in the alphabet depending on the corresponding letter in the key. The key is a repeating keyword, which is interwoven with the plaintext to create the ciphertext. The Vigenère cipher was invented in the 16th century by Giovan Battista Bellaso and later improved by Blaise de Vigenère in the 19th century. The Playfair cipher is another polygraphic substitution cipher, invented by Charles Wheatstone in 1854. It uses a 5x5 matrix of letters, where each letter is paired with another letter from the matrix. The plaintext is divided into pairs of letters, which are then mapped to their corresponding pairs in the matrix using a set of rules. The key is a keyword that is used to generate the matrix.Both of these ciphers were widely used in the past, but they are now considered relatively weak and easily broken by modern cryptographic techniques. However, they played an important role in the history of cryptography and helped pave the way for more advanced cryptographic systems.

One such system is the Transposition cipher, which is a method of encryption that involves rearranging the letters in the plaintext to create the ciphertext. This can be done in a variety of ways, such as by using a fixed pattern or by using a key to specify the rearrangement. The resulting ciphertext may appear to be random, making it difficult for an attacker to decipher without knowledge of the encryption method. Another related concept is the use of multiple encryption layers or rounds, where each layer or round of encryption is based on a different cryptographic algorithm or key. This can make it more difficult for an attacker to break the encryption, as they would need to break multiple layers of encryption in order to recover the original plaintext. Finally, the concept of interweaving messages or data is also used in some modern cryptographic protocols, such as the TLS protocol used for secure communication over the internet. In TLS, multiple streams of data are interweaved and encrypted using a variety of cryptographic algorithms, making it difficult for an attacker to intercept or modify the data being transmitted[8].

Matrix traversal methods are a type of encryption algorithm that involves using a matrix or grid structure to encrypt plaintext messages. There are several different matrix traversal methods used in cryptography, including:

Columnar Transposition: This method involves writing the plaintext message in rows across a matrix, then rearranging the columns of the matrix according to a specific key. The resulting ciphertext is read out by column, rather than by row. Rail Fence: This method involves writing the plaintext message diagonally across a matrix in a "zigzag" pattern, then reading out the ciphertext row by row. The key for this method is the number of "rails" or rows used in the matrix[9].

Playfair Cipher: This method uses a 5x5 matrix of letters, where each letter is paired with another letter from the matrix. The plaintext is divided into pairs of letters, which are then mapped to their corresponding pairs in the matrix using a set of rules[10].
Hill Cipher: This method uses a matrix of numbers instead of letters, and the matrix is multiplied with the plaintext message to produce the ciphertext[11]. The key for this method is the matrix used for multiplication.
Row Transposition: This method involves writing the plaintext message in rows across a matrix, then rearranging the rows of the matrix according to a specific key. The resulting ciphertext is read out by row, rather than by column. Matrix traversal methods can be effective for encrypting messages, but they can also be vulnerable to certain types of attacks. For example, the Playfair Cipher is vulnerable to known plaintext attacks, where an attacker has access to both the plaintext and ciphertext for a given message. Additionally, matrix traversal methods may not be as secure as more modern encryption methods, such as those based on the Advanced Encryption Standard (AES). Encryption and decryption algorithms are mathematical procedures used to transform plaintext into ciphertext (encryption) and transform ciphertext back into plaintext (decryption). These algorithms are essential to modern cryptography, allowing for secure communication and data protection. There are many different encryption and decryption algorithms, each with their own strengths and weaknesses. Some of the most common algorithms include:
Advanced Encryption Standard (AES): This is a symmetric encryption algorithm that is widely used for encrypting data. It uses a block cipher with a variable-length key (128, 192, or 256 bits) and operates on 128-bit blocks of data.RSA: This is an asymmetric encryption algorithm that is widely used for secure communication and digital signatures. It uses a pair of keys (public and private) to encrypt and decrypt data can also be used for digital signatures.
Blowfish: This is a symmetric encryption algorithm that is designed to be very fast and efficient. It uses a variable-length key (up to 448 bits) and operates on 64-bit blocks of data.
DES: This is a symmetric encryption algorithm that was widely used in the past but has since been replaced by AES. It uses a 56-bit key and operates on 64-bit blocks of data.
Diffie-Hellman Key Exchange: This is an asymmetric encryption algorithm that is used to establish a shared secret key between two parties without transmitting the key directly. It is widely used in secure communication protocols such as SSL/TLS.
ElGamal: This is an asymmetric encryption algorithm that is based on the Diffie-Hellman Key Exchange. It uses a pair of keys (public and private) to encrypt and decrypt data and can also be used for digital signatures. There are many other encryption and decryption algorithms as well, and new algorithms are constantly being developed to keep up with advances in computing technology and to address new security threats[12].

## 3. RESEARCH METHOD

The objective of this paper is to propose a new cryptographic scheme. The algorithm uses a random matrix generator that returns an integer matrix, used as a session key in the beginning of each session. For each message to be sent a message key is generated. The message key consists of four parameters row, column, length of the message and traversal method. The message along with the session key and message key is input to encryption method.The method extracts the subkey from the session key based on message key value. The plaintext is converted into their unicode values and arranged in the form of a square matrix based on the traversal method in the message key. The elements of the plaintext matrix are then xor-ed with the corresponding elements of the subkey. The resultant matrix is read horizontally row-wise, and each integer is converted into character equivalent resulting in the ciphertext[13].

### 3.1. Traversal Methods

There are four traversal methods defined in this algorithm which are spiral traversal, diagonal traversal, ascending traversal and descending traversal[14].
Spiral Traversal: The character of plaintext is placed in a square matrix spirally moving first from left to right, top to bottom, right to left, bottom to top and repeat the traversal[15][16].
Example- plaintext: ABCDEFGHIJK,
unicode: 65 66 67 68 69 70 71 72 73 74 75

Plain text matrix using spiral traversal,

$$\begin{bmatrix} 65 & 66 & 67 & 68 \\ 0 & 0 & 0 & 69 \\ 75 & 0 & 0 & 70 \\ 74 & 73 & 72 & 71 \end{bmatrix}$$

Diagonal Traversal: The plaintext characters are arranged diagonally from starting from the primary diagonal, followed by the diagonals to the right and finally all diagonals to the left of the primary diagonal[17].
Example- plaintext: ABCDEFGHIJK,
unicode: 65 66 67 68 69 70 71 72 73 74 75

Plain text matrix using diagonal traversal,

$$\begin{bmatrix} 65 & 69 & 72 & 74 \\ 75 & 66 & 70 & 73 \\ 0 & 0 & 67 & 71 \\ 0 & 0 & 0 & 68 \end{bmatrix}$$

Ascending Traversal: This traversal method will arrange the plaintext characters in a square matrix by traversing through the elements of subkey in ascending order. The first character is placed in the position corresponding to the smallest element of the subkey, the second character in the position corresponding to the next smallest element and so on [18].
Example- plaintext: ABCDEFGHIJK

subkey

$$\begin{bmatrix} 252 & 650 & 202 & 518 \\ 859 & 964 & 925 & 669 \\ 527 & 379 & 662 & 732 \\ 771 & 709 & 800 & 79 \end{bmatrix}$$

Smallest element of subkey is 79 at position (3,3) so the Unicode of the plaintext character A that is 65 is placed in position (3,3) of textmatrix. The next character of plaintext is placed in position corresponding to the position of the next smallest element of subkey and so on.
resultant textmatrix:

$$\begin{bmatrix} 67 & 71 & 66 & 68 \\ 0 & 0 & 0 & 73 \\ 70 & 68 & 72 & 71 \\ 0 & 74 & 0 & 65 \end{bmatrix}$$

Descending Traversal: This traversal is similar to the ascending traversal except that the plaintext characters will be placed in a square matrix by traversing through the elements of subkey in the descending order. The first character is placed in the position corresponding to the largest element of the subkey, the second character in the position corresponding to the next largest element and so on [19][21].
Example- plaintext: ABCDEFGHIJK

subkey

$$\begin{bmatrix} 252 & 650 & 202 & 518 \\ 859 & 964 & 925 & 669 \\ 527 & 379 & 662 & 732 \\ 771 & 709 & 800 & 79 \end{bmatrix}$$

Largest element of subkey is 964 at position (1,1) so the Unicode of the character A that is 65 is placed in position (1,1) of the textmatrix. The next character of plaintext is placed in position as the position of the next largest element of subkey and so on resulting in the textmatrix.

$$\begin{bmatrix} 0 & 74 & 0 & 0 \\ 67 & 65 & 66 & 72 \\ 75 & 0 & 73 & 70 \\ 69 & 71 & 68 & 0 \end{bmatrix}$$

### 3.2. Key Generation

Session Key: The session key is generated using random number generator that generates a random number from 0 to 1000 and placing the number in a matrix of size 10X10. To ensure that no number is repeated python's built-in function for sampling is used.

Message Key: The message key is of the format [row, column, length, traversal method]. [22]This key is generated for each plaintext. The row and column value of the key is randomly selected from numbers 0 to 9 which corresponds to the index of an element in the session key. The length is assigned value of plaintext length. The traversal method is a random number from 0 to 3 where 0 means spiral traversal, 1 means diagonal traversal, 2, is ascending traversal and 3 corresponds to the descending traversal.

Subkey: The subkey is a submatrix that is extracted from the session key starting from the element defined in the message key. Subkey generator will extract elements of session key and place them in a new square matrix of size equal to the ceil of the square root of the length of the plaintext.

**Algorithm:** The client initiating the communication generates a session key and shares it with the receiver. Session key will be secured using existing public key cryptography and sent across the network[23].

**Encryption:**

Step1 Sender writes a message to send, which forms the plaintext.

Step2 Message key is generated for the given plaintext.

i) Randomly choose two digits between 0 and 9 corresponding to row, column values in the message key.

ii) Obtain length of the plaintext.

iii) Choose a digit from 0-3 randomly corresponding to the traversal_method.

iv) Message Key <- [row, column, length, travesal_method]

Step3 Extract subkey from session key using above the generated message key.

Step4 Arrange the plaintext in form of a matrix of dimension same as the subkey using the traversal method specified in the message key.

Step5 XOR the corresponding elements of the subkey and the plaintext matrix.

Step6 Read the resultant matrix row-wise converting the integer into character to obtain the ciphertext.

**Decryption:**

Step1 The message key and the message is received by the receiver.

Step2 Subkey is extracted from the session key using the message key.

Step3 Arrange the ciphertext in form of a matrix, in row-wise manner, of dimension same as the subkey.

Step4 XOR the corresponding elements of the subkey and the ciphertext matrix.

Step5 Read the resultant matrix in accordance with the traversal method specified in the message key to obtain the plaintext.

## 4. RESULTS AND DISCUSSION

Cryptographic interweaving of messages is a technique that is used to protect the confidentiality of messages by combining them in a way that makes it difficult for an eavesdropper to decipher them. This technique involves combining two or more messages in such a way that the resulting ciphertext is a combination of both messages, making it difficult for anyone to separate them. One of the advantages of cryptographic interweaving is that it can be used to provide a higher level of security than traditional encryption techniques. Since the resulting ciphertext is a combination of two or more messages, it is much more difficult for an eavesdropper to determine the contents of any single message.

The following example is explaining data encryption and decryption meethods of proposed techniques.

Session key matrix,

$$\begin{bmatrix} 925 & 669 & 226 & 402 & 552 & 907 & 14 & 332 & 859 & 964 \\ 662 & 732 & 485 & 10 & 987 & 639 & 955 & 502 & 527 & 379 \\ 800 & 79 & 212 & 310 & 440 & 863 & 816 & 508 & 771 & 709 \\ 447 & 75 & 176 & 722 & 74 & 640 & 564 & 730 & 757 & 826 \\ 787 & 256 & 29 & 371 & 799 & 151 & 702 & 72 & 108 & 410 \\ 373 & 197 & 235 & 12 & 531 & 150 & 475 & 282 & 773 & 603 \\ 179 & 136 & 546 & 577 & 901 & 493 & 565 & 541 & 941 & 398 \\ 857 & 455 & 122 & 95 & 848 & 309 & 12 & 472 & 734 & 572 \\ 887 & 718 & 258 & 335 & 415 & 947 & 632 & 896 & 981 & 366 \\ 202 & 518 & 596 & 971 & 551 & 124 & 585 & 608 & 252 & 650 \end{bmatrix}$$

Encryption:
Plaintext: cryptography
Message Key: [9, 8, 12, 2]
Subkey:

$$\begin{bmatrix} 252 & 650 & 202 & 518 \\ 859 & 964 & 925 & 669 \\ 527 & 379 & 662 & 732 \\ 771 & 709 & 800 & 79 \end{bmatrix}$$

The unicode value of each alphabet in the word ‘cryptography’ is,

| c | r | y | p | t | o | g | r | a | p | h | y |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 99 | 114 | 121 | 112 | 116 | 111 | 103 | 114 | 97 | 112 | 104 | 121 |

In this example, the fourth parameter of the message key is 2, i.e the traversal is in the ascending order. The plain text matrix is obtained by arranging these unicode values in a matrix in an order thats maps to the ascending order of traversal in subkey (Eg: 79,202,252, so on)
Plain text matrix,

$$\begin{bmatrix} 121 & 103 & 114 & 116 \\ 0 & 0 & 0 & 97 \\ 111 & 112 & 114 & 104 \\ 121 & 112 & 0 & 99 \end{bmatrix}$$

An XOR operation is performed between subkey and the plaintext matrix to obtain the ciphertext matrix.
$S \oplus P = C =$

$$\begin{bmatrix} 133 & 749 & 184 & 626 \\ 859 & 964 & 925 & 764 \\ 608 & 267 & 740 & 692 \\ 890 & 693 & 800 & 44 \end{bmatrix}$$

The ciphertext matrix is then read horizontally and each value is converted into its corresponding character value to obtain the ciphertext.
Cipher text: ‟,”zzguzjuvbzjgivbigszb”
Decryption Cipher text: ‟ “Hello World”,
Message Key: [9, 8, 12, 2]
Subkey S =

$$\begin{bmatrix} 252 & 650 & 202 & 518 \\ 859 & 964 & 925 & 669 \\ 527 & 379 & 662 & 732 \\ 771 & 709 & 800 & 79 \end{bmatrix}$$

The ciphertext characters are converted into their unicode values and these values are inserted horizontally into a matrix i.e ciphertext matrix.

C =

$$\begin{bmatrix} 133 & 749 & 184 & 626 \\ 859 & 964 & 925 & 764 \\ 608 & 267 & 740 & 692 \\ 890 & 693 & 800 & 44 \end{bmatrix}$$

XOR operation is performed between the subkey and the ciphertext matrix.
The resultant matrix is the plaintext matrix.
S $\oplus$ C = P =

$$\begin{bmatrix} 121 & 103 & 114 & 116 \\ 0 & 0 & 0 & 97 \\ 111 & 112 & 114 & 104 \\ 121 & 112 & 0 & 99 \end{bmatrix}$$

Finally, the plaintext matrix is read in ascending (specified traversal) order of traversal corresponding to the values in the subkey matrix to obtain the plaintext. Plaintext: cryptography

Security Analysis:
The subkey consists of randomly generated non-repeating and non-negative integers used for encrypting the messages. Hence, the numerous permutations of the plaintext obtained weakens the probability of deciphering the plaintext by mere brute force attack. The plaintext characters are shuffled based on the traversal type and different ciphertext characters are obtained for same plaintext characters. [24] Hence, frequency attack becomes difficult. We are using different subkey for each message. So even the known plaintext attack of one message's result won't affect the other messages. [25] The coding gain of the proposed scheme has been verified, via a proof-of-concept experiment.

Comparative Study:
The widely used algorithms like AES, DES, etc involve multiple (10-16) rounds of processing, requiring high computation. Whereas this algorithm involves very little computation thereby reducing the computational overhead. Also, its symmetric nature overcomes the need of establishment of a strong mathematical relation between the public and the private key like the RSA algorithm. [26] [27] The key matrix in our algorithm can be any sequence of numbers unlike in Hill Cipher where only the matrix with nonzero determinant can be used.

## 5. CONCLUSION

The proposed algorithm can be used by any application which involves transmission of text messages. Therefore, this algorithm can find use in, e-transaction, e-message and information storage. It supports message transfer in all the languages supported by the unicode system. Randomness of the keys, their arrangement in the form of two-dimensional matrices and the various possible traversal techniques, ensures multiple level of security and contents [29]. The encryption executes either redundant precoding or FTN signaling [29] , which can increase security performance while regulating total data throughput. Despite the fact that transmission performance and security performance are tradeoffs [30]. The algorithm is flexible enough to incorporate numerous other traversal techniques. The two-dimensional matrix concept can be extended to a three-dimensional matrix by arranging the matrix contents in a 3D plane instead of 2D plane. A selection can be made between whether to choose a 2d or a 3d matrix operation, based on the size of the plaintext thereby reducing the need of padding it with extra bits. Also, traversals can be based on sharing the coordinates of the content of the two/three-dimensional matrix. The challenge could be the minimization of the overhead involved.

## REFERENCES

[1] Nadeem, M., Arshad, A., Riaz, S., Zahra, S. W., Dutta, A. K., Al Moteri, M., & Almotairi, S. (2022). An Efficient Technique to Prevent Data Misuse with Matrix Cipher Encryption Algorithms. Comput. Mater. Contin, 74, 4059-4079.
[2] Krishna, A. V. N., Pandit, S. N. N., & Babu, A. V. (2007). A generalized scheme for data encryption technique using a randomized matrix key. Journal of Discrete Mathematical Sciences and Cryptography, 10(1), 73-81.
[3] Ratha, P., Swain, D., Paikaray, B., & Sahoo, S. (2015). An optimized encryption technique using an arbitrary matrix with probabilistic encryption. Procedia Computer Science, 57, 1235-1241.
[4] Nath, A., Ghosh, S., & Mallick, M. A. (2010, July). Symmetric Key Cryptography Using Random Key Generator. In Security and Management (pp. 234-242).
[5] Hamamreh, R., & Farajallah, M. (2009). Design of a robust cryptosystem algorithm for non-invertible matrices based on hill cipher.

[6] Gitanjali, J., Jeyanthi, N., Ranichandra, C., & Pounambal, M. (2014, June). ASCII based cryptography using unique id, matrix multiplication and palindrome number. In The 2014 International Symposium on Networks, Computers and Communications (pp. 1-3). IEEE.
[7] Alkim, E., Ducas, L., Pöppelmann, T., & Schwabe, P. (2016, August). Post-quantum key exchange-A New Hope. In USENIX security symposium (Vol. 2016).
[8] Mikhail, J. A., & Keith, B. F. (2010, April). Securely outsourcing linear algebra computations. In Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security. ACM.
[9] Bunch, J. R., & Rose, D. J. (Eds.). (2014). Sparse matrix computations. Academic Press.
[10] Bai, Z., Fahey, G., & Golub, G. (1996). Some large-scale matrix computation problems. Journal of Computational and Applied Mathematics, 74(1-2), 71-89.
[11] Benjamin, D., & Atallah, M. J. (2008, October). Private and cheating-free outsourcing of algebraic computations. In 2008 Sixth Annual Conference on Privacy, Security and Trust (pp. 240-245). IEEE.
[12] Van Waarde, H. J., Camlibel, M. K., Rapisarda, P., & Trentelman, H. L. (2022). Data-driven dissipativity analysis: application of the matrix S-lemma. IEEE Control Systems Magazine, 42(3), 140-149.
[13] Bai, Z. Z., & Pan, J. Y. (2021). Matrix analysis and computations. Society for Industrial and Applied Mathematics.
[14] Boneh, D., Goh, E. J., & Nissim, K. (2005, February). Evaluating 2-DNF Formulas on Ciphertexts. In TCC (Vol. 3378, pp. 325-341).
[15] Krendelev, S. F., Yakovlev, M., & Usoltseva, M. (2014, September). Order-preserving encryption schemes based on arithmetic coding and matrices. In 2014 Federated Conference on Computer Science and Information Systems (pp. 891-899). IEEE.
[16] Dong, T., Wang, Y., & Lei, L. (2018, December). A File Encryption Algorithm Based on Dynamic Block Out of order Matrix Mapping. In 2018 International Conference on Security, Pattern Analysis, and Cybernetics (SPAC) (pp. 246-248). IEEE.
[17] Chang, W. T., & Tandon, R. (2018, December). On the capacity of secure distributed matrix multiplication. In 2018 IEEE Global Communications Conference (GLOBECOM) (pp. 1-6). IEEE.
[18] Rajesh, N., Selvakumar, A.A.L. Association rules and deep learning for cryptographic algorithm in privacy preserving data mining. Cluster Comput 22 (Suppl 1), 119–131 (2019). https://doi.org/10.1007/s10586-018-1827-6
[19] Zhang, S., Tian, C., Zhang, H., Yu, J., & Li, F. (2019). Practical and secure outsourcing algorithms of matrix operations based on a novel matrix encryption method. IEEE Access, 7, 53823-53838.
[20] Hu, Z., & Chan, C. K. (2018). A real-valued chaotic orthogonal matrix transform-based encryption for OFDM-PON. IEEE Photonics Technology Letters, 30(16), 1455-1458.
[21] Simon, W. A., Qureshi, Y. M., Rios, M., Levisse, A., Zapater, M., & Atienza, D. (2020). BLADE: An in-cache computing architecture for edge devices. IEEE Transactions on Computers, 69(9), 1349-1363.
[22] Gao, K., Horng, J. H., & Chang, C. C. (2021). An authenticatable (2, 3) secret sharing scheme using meaningful share images based on hybrid fractal matrix. IEEE access, 9, 50112-50125.
[23] Yu, N. Y. (2017). Indistinguishability of Compressed Encryption with Circulant Matrices for Wireless Security (vol 24, pg 181, 2017). IEEE SIGNAL PROCESSING LETTERS, 24(7), 1098-1098.
[24] Zhang, T., Lu, H., & Liu, X. Y. (2020). High-Performance Homomorphic Matrix Completion on Multiple GPUs. IEEE Access, 8, 25395-25406.
[25] Prabhdeep Singh, & Ashish Kumar Pandey. (2022). A Review on Cloud Data Security Challenges and existing Countermeasures in Cloud Computing. International Journal of Data Informatics and Intelligent Computing, 1(2), 23–33. https://doi.org/10.5281/zenodo.7464700
[26] Pistono, M., Bellafqira, R., & Coatrieux, G. (2021). Cryptosystem Conversion, Packing and Matrix Processing of Homomorphically Encrypted Data: Application to IOT Devices. IEEE Access, 9, 28302-28316.
[27] Hu, Z., Song, P., & Chan, C. K. (2021). Chaotic non-orthogonal matrix-based encryption for secure OFDM-PONs. IEEE Photonics Technology Letters, 33(20), 1127-1130.
[28] Cvijetic, N. (2011). OFDM for next-generation optical access networks. Journal of lightwave technology, 30(4), 384-398.
[29] Chow, C. W., Yeh, C. H., Wang, C. H., Shih, F. Y., Pan, C. L., & Chi, S. (2008). WDM extended reach passive optical networks using OFDM-QAM. Optics Express, 16(16), 12096-12101.
[30] Chow, C. W., Yeh, C. H., Wang, C. H., Wu, C. L., Chi, S., & Lin, C. (2010). Studies of OFDM signal for broadband optical access networks. IEEE Journal on Selected Areas in Communications, 28(6), 800-807.

## BIOGRAPHIES OF AUTHORS

**Jagadeesh Sai D** was with ADP from 2006 to 2008. he got M.Tech degree in Computer science and Engineering at Jawaharlal Nehru Technological University in 2014. He became an Assistant Professor in 2011, currently working as research scholor in Ramaiah Institute of technology. His current research interests include Secure distributed systems and crypotography its applications such as in cloud data security and novel encryption techniques. He has published more than 18 journal papers in the fields of Computer science and its applications. He can be contacted at email: djsai@msrit.edu

**Krishna Raj P. M**. received the Ph.D. degree in Computer Science and Engineering. He has been an associate professor of information Scine & Engineering in Ramaiah Institute of Technology, since 2004. He is currently the IT coordinator of Ramaig Institute of technogy and Gokula educational. He has authored or coauthored more than 40 refereed journal and conference papers, 38 book chapters, and three edited books with Elsevier and Springer. His research interests include the applications of artificial intelligence, He is interested in subjects related to philosophy of technology and aesthetic computing. He can be contacted at email: krishnarajpm@msrit.edu