IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-6, June 2018 E-ISSN: 2347-2693

A Hybrid Multi-Stage Methodology for Secure Outsourcing of Confidential Data to Public Cloud

Konakanti Bhargavi [1*], Thota. Bhaskara Reddy[2]

[1]Department of Computer Science and Engineering, JNTU, Anantapur, India
[2]Department in computer science and technology, Sri Krishna Devaraya University, Anantapur, India

** Corresponding author E-mail: bhargavikonakanti@gmail.com*

Available online at: www.ijcseonline.org

Accepted: 10/Jun/2018, Published: 30/Jun/2018

Abstract-- Cloud is the Internet based computing that provides resources on-demand. This has become an attractive solution to data owners as the can outsource data and computing. There is potential risk in terms of security and privacy of the outsourced data as the cloud servers are treated untrusted. In this context, there are two security mechanisms that are widely used. They are known as cryptography and steganography. The cryptography converts data into some format that cannot be comprehended by humans while the steganography hides the presence of a message (may be encrypted one) in an image or any digital media. If both are used independently they have their own limitations. When both are combined, it forms a realizable mechanism with both security and secrecy. Thus, the Crypto-steganography is the approach that overcomes the limitations of individual mechanisms as it proves to be difficult to adversaries to launch attacks. In this paper an LSB substitution method and quadruple efficient image encryption method are used to secure sensitive messages when they are outsourced to public cloud. We built a prototype application to show the utility of the proposed hybrid method. The results revealed that the proposed is capable of increasing security to the data outsourced to public cloud.

Keywords **–** Cloud computing, cryptography, steganography, crypto-steganography

I. INTRODUCTION

Due to the innovative technologies emerged in the real world, the way computing takes place is made different. Now it is possible to have Internet computing. It is a phenomenon through which storage and computation takes place in remote computers. An individual can use a PC or laptop with Internet connection to connect to cloud and perform data dynamics. With the availability of smart phones and their increased capabilities, people of all walks of life started using them and sending their data to cloud. In this context, cloud usage became more with respect to individuals and organizations [1]. When data is stored in public cloud, it is accessible from anywhere in the world. It removes barriers like geography and time. Without restrictions, the data owners can gain access to such data for 365 days. In addition to this, cloud computing allows users to have many benefits like affordable storage space and other services. Cloud provides inexhaustible resources that are scalable. Thus outsourcing data to public cloud became very popular use case with respect to cloud computing.

Cloud resources are provisioned on demand. Especially its storage and computing services are widely used by people and organizations [2]. The storage in public cloud may have multimedia content. Often it is known as big data with characteristics like volume (huge amount of data is outsourced), variety such as structured, unstructured and semi-structured data and velocity indicating that the data is streamed continuously and growing exponentially. Though cloud service providers (CSPs) claim that they provide privacy and security to outsourced data, the cloud servers are treated untrusted by the data owners who outsource data. That is the reason why data owners try to provide security to their data before outsourcing to public cloud. For instance, data owners may encrypt data and outsource it. Thus they ensure that their data is protected and not misused by adversaries. There are some instances that proved to be potential risk to public data as explored in [3]. Many solutions came into existence to solve the problems of data security and privacy in public cloud. The research found in the literature include image transmission with encryption [4], generation of credentials dynamically [5] and secret image sharing [6] to mention few. In the literature it is found that usage of cryptography and steganography independently do have their limitations. To overcome this limitation, in this paper, we proposed a methodology to combine them in the form of crypto-steganography to achieve both data security and secret sharing of data. Thus it allows confidential data to be

outsourced to public cloud without compromising security. Our contributions are as follows.

- We proposed a methodology that facilitates the usage of cryptography and steganography to have data security and secret sharing of confidential information. Sensitive content is encrypted and enclosed in stego image before outsourcing it to public cloud.
- We built a prototype application to demonstrate proof of the concept. The experimental results revealed that the proposed method is effecting in securing data and sharing it with secrecy with respect to outsourcing data to public cloud.

The remainder of this paper is organized as follows. Section II is the literature review of combining cryptography and steganography. Section III explains the proposed work. Section IV shows the experimental results while conclusion is provided in section V.

II. RELATED WORK

This section reviews literature on the security and secret sharing mechanisms. A mechanism is proposed in [7] for steganography using visual cryptography and neural network. Visual cryptography is well known technique to protect text or images by using multimedia object as cover. They divided cover image into number of blocks and made energy efficient approach. Best locations in the cover image are identified by using neural network while LSB embedding is employed to embed text into image. In [8] on the other hand a technique is proposed to protect images. The image that needs to be communicated with secrecy is embedded into cover image. They used LSB technique in the spatial domain. Afterwards, the image is subjected to 8*8 division of blocks. Then the divided image is subjected to encryption with the help of double random phase encoding resulting into white stationary noise.

In [9] Internet of Things (IoT) environment is used to have secure data transfer. Towards this end, they proposed a technique known as steganography and cryptography when data is being transferred among IoT devices. IoT sensor senses data and such data is encrypted and embedded into a stego image in order to have secure communication. Before embedding the message's message digest is computed and encrypted. The message digest is used by both sender and receiver to know the integrity of data transferred. Authors in [10] used RSA algorithm and audio steganography. RSA is used for encryption while the LSB audio technique is used to hide the encrypted text into stego image. In [11] gray images are used with both cryptography and steganography. Here vernam cipher is used to encrypt secret image. After encryption, the message is embedded into a cover image using LSB with shifting techniques. On the other hand in [12] two approaches are used for secure data transfer. In the first technique secret image is considered and encrypted using cryptographic technique known as S-DES algorithm for generating encrypted pixels. Afterwards the elements of array are divided into 4 MSBs and remaining LSBs. The pixel value is then converted into alphabets containing characters from A to P corresponding to values 0000 to 1111. The output of the operation is an encrypted image that is embedded into a cover image with the help of XOR method. The second method is to have simple encryption of secret image using S-DES.

In [13] a hybrid approach is used to have good encryption quality. Blowfish algorithm is used to encrpt given secret image and generates a cipher image. Then the encrypted image is embedded into a cover image using LSB method. The approach is lossless and provides high level of security. In [14] a method is proposed to combine both cryptography and steganography. However, the cover media taken is MP3 file. AES is used for encryption and MD5 hash function is also used. The encrypted image is embedded into cover medium. The cover image and secret image are considered with same size in [15]. For both images a single plane is considered. The secret image is dividing into a set of 16 pixels and they are converted to cipher text before embedding.

Security of file system in cloud computing is explored in [16]. The cloud computing adoption by organizations is investigated in [17]. In the cloud storage, image encryption with private key encryption is studied in [18] while various cloud scenarios is studied in [19]. Cryptography for data storage in cloud computing and authentication models for secure cloud access are reviewed in [20] and [21] respectively. As found in the literature there are many contributions related to cryptography and steganography. In this paper we proposed a methodology that can help in using both cryptography and steganography to have high quality of images and less time complexity.

III. OUR METHODOLOGY

The methodology we proposed has two important activities. The first activity is related to cryptography while the second one is related to steganography. To have more security, it is important to embed secret text into images after encryption. That is the reason encryption is made before secret text embedding into cover mage.

A. Secret Text Preparation

The secret text that is to be outsourced to public cloud is taken and it is subjected to transformation using

cryptography. Encoding the secret text is the purpose of the activity so as to allow only authorized parties to gain access to it. A four stage encryption process is employed here. The four stages are known as Zig-Zag scan, rail fence, crossover and Xor.

Zig-Zag scan: This operation is used to identify low-frequency coefficients and group them into a vector. It is nothing but transform based coding. It is best used for N x N DCT coefficients with non-uniform quantization. As I is very sensitive to low frequencies and sensitive in case of high frequencies, lower frequencies are considered to have most of the energy. The result of the operation is to have ID sequence and number of non-zero coefficients and remaining values to be zero. Zig Zag scan operates on the binary numbers. However, in the proposed method, it is made to work on the decimal numbers. The original text is converted to un-understandable format. As it groups low-frequency coefficients, the result is a matrix with either 8 x 8 or 4 x 4 size. It generates intermediate results as follows.

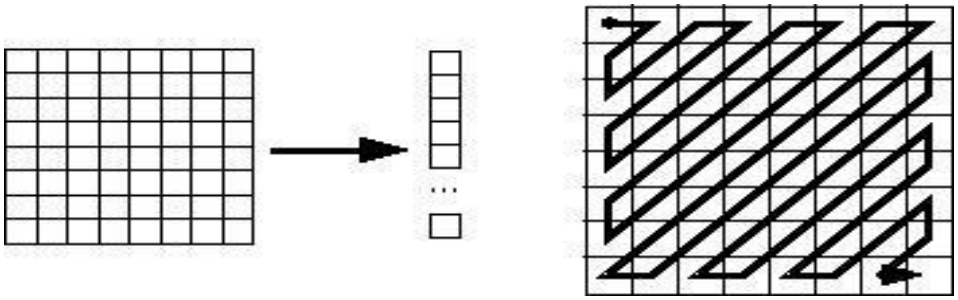

Figure 1: Zig Zag scan matrix of 8 x 8 sizes

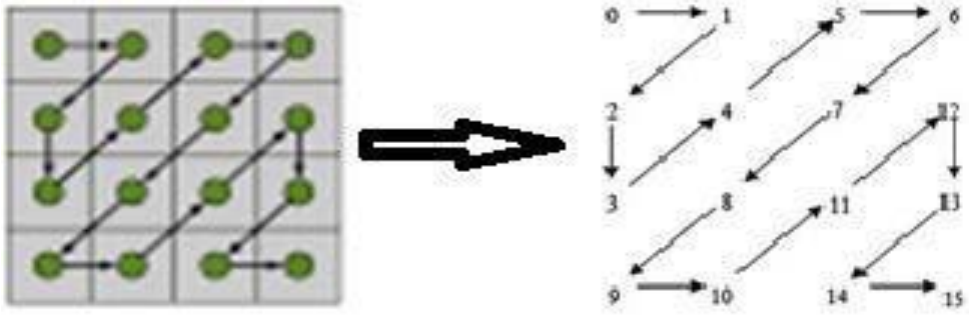

Figure 2: Zig Zag matrix of size 4 x 4

As presented in Figure 2, it is evident that the matrices with 8 x 8 and 4 x 4 size are generated with the help of Zig Zag scanning. This operation, in other words, produced intermediate results.

Rail Fence: After completion of Zig Zag scan, the method known as Rail Fence is carried out. It is called Zig Zag cryptography. It is one of the examples of transposition ciphers. Here the plaintext elements are converted to a matrix which is used by sender and receiver. As explored in [7] and [8] there are many ways in which cipher text can be created. It can also be used to perform diagonal retrieval. However, cipher security with Rail Fence is very week. The reason behind this is that it does not use a key. It can break adversaries easily. It helps in mixing up characters of plaintext in order to generate cipher text. It does not provide good communication security. Therefore, it cannot be directly used to encrypt images. Example of this method is illustrated in Figure 3.

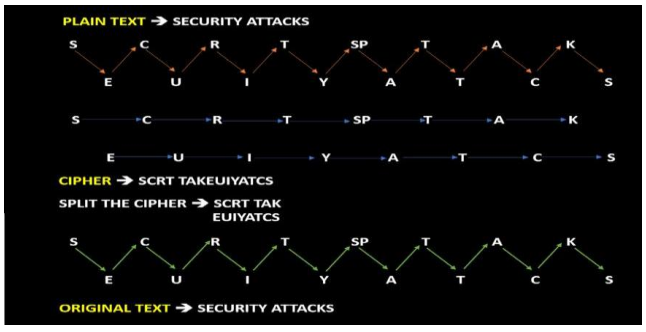

Figure 3: Illustrates rail fence mechanism

Figure 3: Illustrates rail fence mechanism

As presented in Figure 3, it is evident that data is organized in the form of waves with two levels of values. First level values

follow second level values in order to have intermediate cipher text. After this, the intermediate cipher is split into two parts in order to develop rail fence structure. Performing rail fence mechanism on this will produce original text.

Crossover: This operator is similar to reproduction and looks like biological crossover. Here multiple parents are chosen to have off-springs production by considering genetic content of parents. It is to be understood that the crossover operation is very generic and it is possible to have GA design to be more specific to problem area. There are different types of crossover functions. They are known as one point crossover, multipoint crossover, and uniform crossover and modified crossover. They are as illustrated in Figure 4.

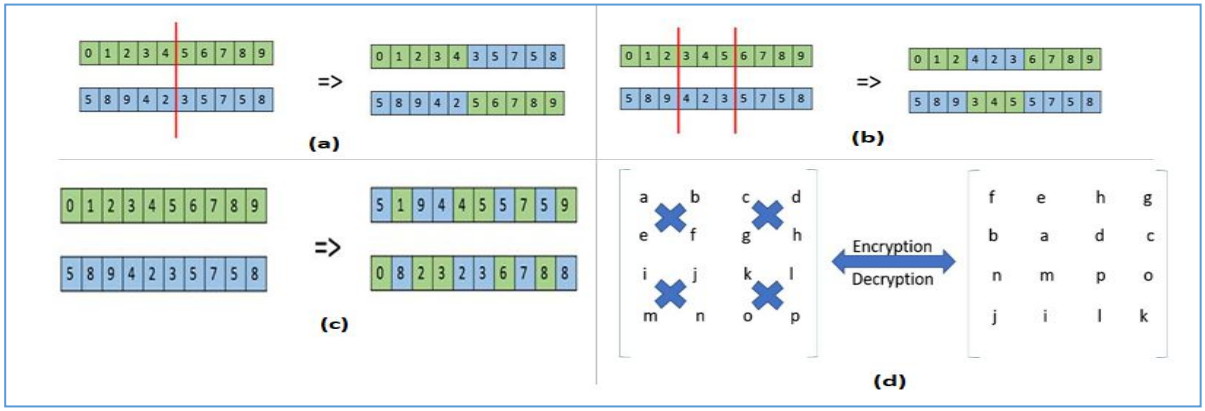

Figure 4: Different types of crossover operations a) one-point crossover b) multi-point crossover c) uniform crossover d) modified crossover

In case of one-point crossover, selection of random crossover point is made besides swapping tails of two parents in order to obtain new off-springs. In case of multi-point crossover, as it is nothing but the generalization of one-point crossover, swapping of alternating segments is made in order to obtain new off-springs. With respect to uniform crossover, the chromosomes are not divided into segments as each gene is treated separately. For each chromosome there is flipping of coin and to decide to be included in the off-spring or not. It is also possible to have more genetic material by biasing the coin with respect to child in the corresponding parent. The proposed method employs new crossover technique that can convert original matrix into some intermediate cipher text.

XOR Operation: It is very common operation in case of complex ciphers. It is easier to use and computationally inexpensive. A repeating XOR can provide cipher that is used to secure data. By using a constant repeating key, it is possible to have broken with the help of frequency analysis. When the key is random and it is long as the message, then the XOR cipher is better used as it renders high level of security. As all computations in computer are done using binary language, the numbers, characters, images and everything is presented in the form of binary value. Just integers are considered here. Before storing integers, computer converts it into binary. In the proposed system 16 is considered as the key in order to perform XOR operation.

B. Protecting Secret Text in Stego Cover Image

Once secret text is created using the procedure described in the previous section, the text is to be embedded into a cover image. In this case, the steganography needs two kinds of data. The first one is known as cover image while the second one is known as data or secret text that is to be secured into the stego image. The cover here is nothing but the medium into which the secret text is embedded. An important feature of cover image is that it supports a variety of colors. When the image contains less number of colors, embedding process is easier to detect. If any image has two colors, then it is very clear that there will be two colors after embedding.

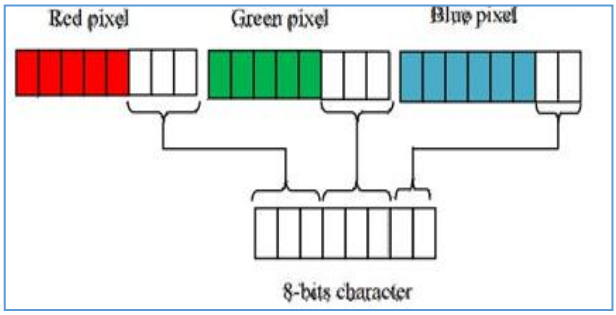

Figure 5: Data embedding in RGB pixels

As presented in Figure 5, data embedding is possible in RGB pixels. There are different approaches to do it. For instance, Least Significant Bit (LSB) is one of the approaches that follow specific procedure to embed data into least significant bits.

C. Least Significant Bit (LSB)

LSB is one of the simple strategies to embed text into images. Like any typical method of steganography, the text is embedded into cover image and it cannot be found by any observer. LSB works replaces information in pixels with the secret data that has been encrypted. It is possible to embed data in any bit plane. But it is understood that LSB considers least significant bits for embedding. This can actually minimizes difference in color of image even after embedding. The color value is changed by one when LSB embedding is performed. When embedding is done with the second bit plane, it is possible to change color value by 2. On the other hand if LSB is used for embedding, the color of the pixel that is used for embedding may use one of the colors. It reduces the likelihood of detecting the stego image. Nevertheless, there is always loss of information in the stego image. The reason behind it is that data is embedded directly into a pixel. This way cover image's information is discarded and replaced by the secret text to be hidden. LSB algorithms are also able to provide choice about embedding process. They can also help in embedding losslessly preserving data and consuming less space.

IV. PROPOSED ALGORITHMS

Algorithms are proposed to perform encryption and embedding effectively. The encryption algorithm is known as Multi-Stage Secret Text Encryption algorithm.

A. Multi-Stage Secret Text Encryption

This algorithm is used to encrypted data that is to be secured and transferred to cloud. In other words, the secret message that needs to be outsourced to cloud is subjected to encryption using this algorithm. The algorithm has multiple phases as described in the section 4.

And Embedding Algorithm

Step 1: Read the text file.
Step 2: Convert each character in the file into corresponding ASCII value.
Step 3: Construct the corresponding data into 4 x 4 matrices.
Step 4: Each 4 x 4 block performs the following method
Step 4.1: Modified 4 x 4 Zig-Zag scan
Step 4.2: Modified Rail fence
Step 4.3: Crossover
Step 4.4: XOR operation
Step 5: Embed the result of XOR into individual RGB planes.

Algorithm 1: Multi-Stage Secret Text Encryption and Embedding

The algorithm takes secret text as input in the form of text file. Then it converts the text into ASCII values. Afterwards a 4x4 matrix is constructed. Then the matrix is subjected to four-phase encryption process. The four phases involved are Zig Zag scan, modified rail fence, crossover and XOR operation. The functionality of this algorithm is illustrated below. In step 1, user selects a text file named message.txt and the data found in the file is "Cyber Security". On converting each character in the given input file into ASCII values, the outcome looks as shown in Figure 6.

C	y	b	e	r		S	e	c	u	r	i	t	y	sp	sp
67	121	98	101	114	32	83	101	99	117	114	105	116	121	32	32

Figure 6: Shows ASCII values of characters

Afterwards, there is construction of 4x4 matrices and ZigZag scan is performed on each block.

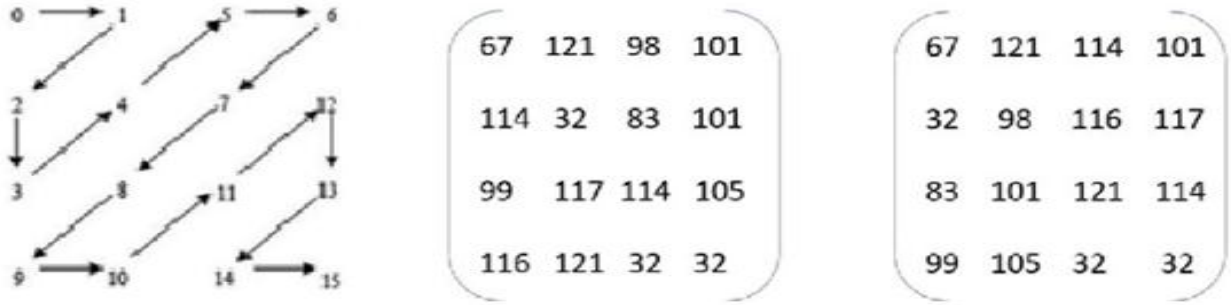

Figure 7: Shows patterns before and zig zag

As shown in Figure 7, it is evident that the Zig zag patern before and after peformng Zig Zag operation. Then he rail fence is

modified and presented dto be part of the ecryption processs. Before exploring modified Rail Fence, it is imprtnat to understand original matrix.

67	114	32	116
83	121	99	32
121	101	98	117
101	114	105	32

Figure 8: The original matrix

As shown in Figure 8, it is evident that matrix is created to reflect the entities in the array. This array is used further to have modified rail fence. Once modified rail fence is employed, the result of are presented as follows.

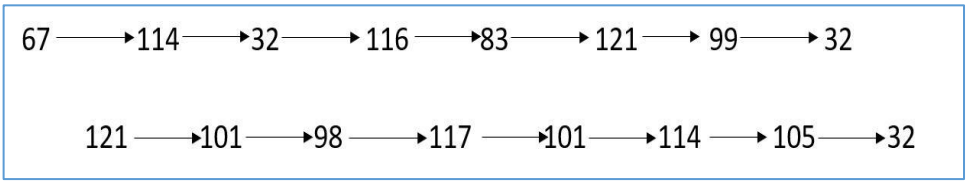

Figure 9: The results of rail fence

As presented in Figure 9, it is evident that there are two set of values provided that are taken from the original matrix. Then the result of crossover is as shown in Figure 10.

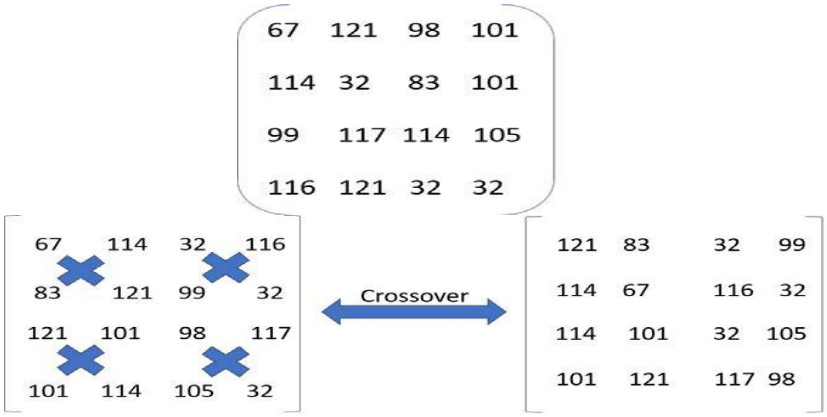

Figure 10: Shows matrix before and after cross over

As shown in Figure 10, it is evident that the matrix shows values that are subjected to cross over in order to generate new values. Then the result is subjected to XOR operation. XOR operation is performed with 16 to all values present in each block.

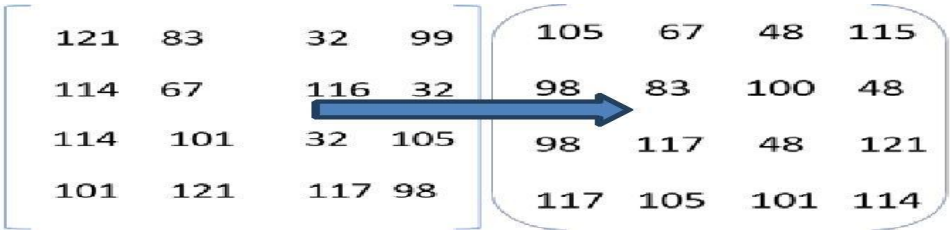

Figure 11: Result before and after performing XOR

As shown in Figure 11, it is evident that the XOR operation is resulted in a new set of values shown. These values are further subjected to encryption.

Figure 12: Shows original message and encrypted message

As shown in Figure 12, the original secret text is encrypted into cipher text. Then the resultant text is embedded into stego image using embedding process.

ASCII	BINARY(ASCII)	RGB BINARY(IMAGE)	EMBED
105	01101001	R=10100011 G=01011100 B=00010111	R=10100011 G=01011010 B=00010101
67	01000011	R=10111001 G=01001000 B=01110101	R=10111010 G=01001000 B=01110111
48	00110000	R=11101011 G=01101110 B=00010011	R=11101001 G=01101100 B=00010000
115	01110011	R=10011000 G=01001100 B=01010010	R=10011011 G=01001100 B=01010011
98	01100010	R=10111010 G=01111101 B=01011100	R=10111011 G=01111000 B=01011110

Figure 13: Results of embedding

As presented in Figure 13, it is evident that the ascidia values are converted to binary values and embedded into appropriate pixel in the stego image.

Figure 14: The original image (left) vs. stego image (right)

The original image is used to embed given text and it is converted into stego image. As shown in Figure 14, the stego image appears similar to the original image for human eye believing that it is just an image. However, secret message is embedded into that image. In order to obtain the secret image, we need to follow procedure.

B. Multi-Stage Secret Text Extraction Algorithm

Decryption is used to obtain the plain text or secret message back. It has certain number of steps.

Step 1: Extract the RGB pixels from the stego image.
Step 2: Convert each pixel into corresponding ASCII value.
Step 3: Construct the corresponding data into 4 x 4 matrices.
Step 4: Each 4 x 4 block performs the following methods one by one
Step 4.1: XOR operation
Step 4.2: Crossover
Step 4.3: Modified Rail fence
Step 4.4: Modified 4 x 4 Zig-Zag scan
Step 5: Decrypted plain.txt file will be created.

Algorithm 2: Multi-Stage Secret Text Extraction and Decryption

When the decryption process is involved, the results are as illustrated in the following example. First of all extracted embedded pixels are collected in order to obtain cipher text from the stego image used in the process of embedding.

RGB EMBEDED BINARY (IMAGE)	CIPHER BINARY(ASCII)
R=10100011 G=01011010 B=00010101	01101001
R=10111010 G=01001000 B=01110111	01000011
R=11101001 G=01101100 B=00010000	00110000
R=10011011 G=01001100 B=01010011	01110011
R=10111011 G=01111000 B=01011110	01100010

Figure 15: Converting pixels into cipher text

As presented in Figure 15, the pixels in the stego image where text is embedded are used to extract cipher text which is nothing but binary values. Then the binary values are converted into the ASCII values as shown in Figure 16.

CIPHER BINARY(ASCII)	ASCII
01101001	105
01000011	67
00110000	48
01110011	115
01100010	98

Figure 16: Converting cipher text into ASCII values

As shown in Figure 16, it is evident that the binary cipher text is converted into ASCII values that represent decimal values associated with original secret message.

105	67	48	115
98	83	100	48
98	117	48	121
117	105	101	114

Figure 17: Resultant 4x4 matrix

As presented in Figure 17, it is evident that the matrix contains decimal values that are associated with the secret text that has been subjected to conversion and embedding. Then the matrix is subjected to XOR operation with 16 to all values in the block. The result is shown in Figure 18.

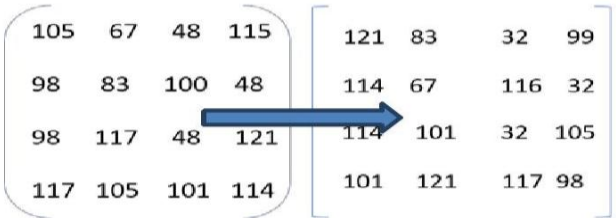

Figure 18: Before and after XOR the data in 4x4 matrix

As presented in Figure 18, the values are presented in 4x4 matrix before XOR operation. The result of XOR operation is also presented in the form of 4x4 matrix. After this the data is subjected to Crossover operation in order to obtain 4x4 matrix.

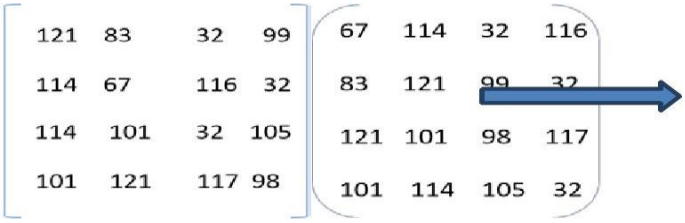

Figure 19: Shows 4x4 matrix before and after Crossover

As presented in Figure 19, the 4x4 matrix is subjected to crossover and the result is shown in another 4x4 matrix. Then the resultant matrix is subjected to modified Rail Fence activity in order to obtain original matrix.

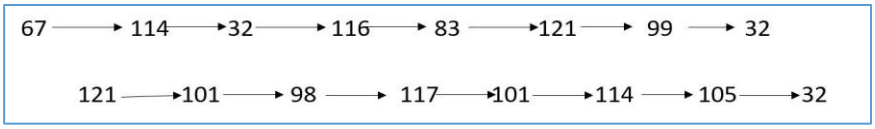

Figure 20: Result of modified Rail Fence operation

The result of the rail fence operation, the values is again represented in the form of 4x4 matrix as shown in Figure 21.

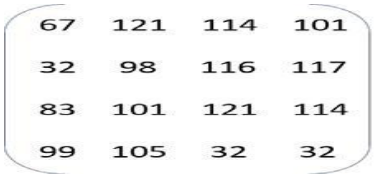

Figure 21: Result of modified Rail Fence operation in the form of 4x4 matrix

Once the modified rail fence operation is carried out, the resultant 4x4 matrix is subjected to Zig Zag scan. The result of this operation is presented in Figure 22.

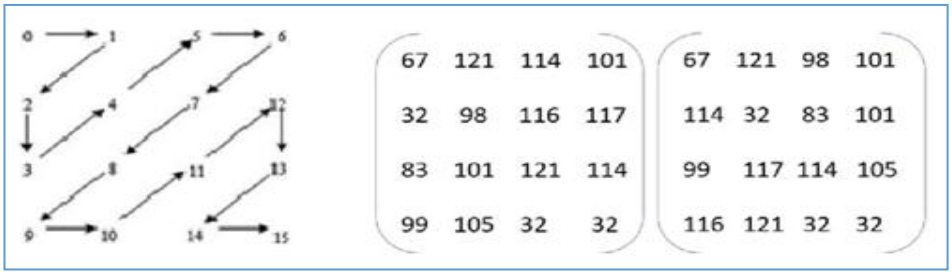

Figure 22: Matrix before and after ZigZag pattern

The ZigZag scan is resulted into the final matrix of 4x4 with original values still not in the form of plain text. Then the decryption process completion is resulted in the form of original secret message.

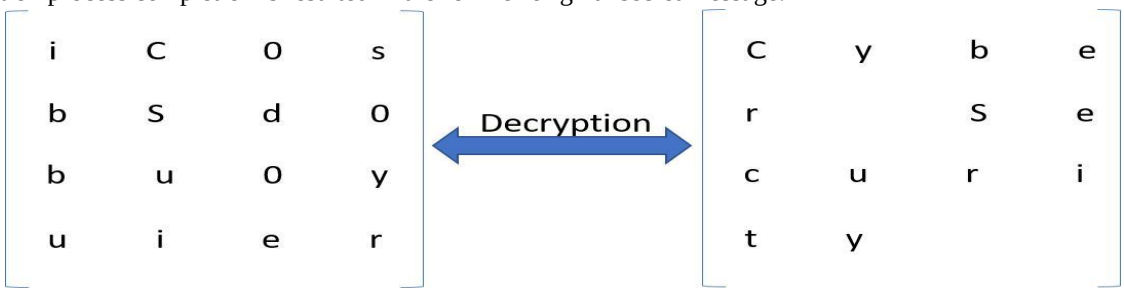

Figure 23: Decryption to obtain original secret message

As presented in Figure 23, it is evident that the original secret message is obtained after decryption process. Thus the proposed methodology provides procedure to have both cryptography and steganography for securing data and secret sharing of data respectively.

V. EXPERIMENTAL RESULTS

Experiments are made to evaluate the proposed methodology with a prototype application. The performance metrics considered are time complexity and PSNR. The results showed the utility of the proposed methodology in secure outsourcing of confidential data to public cloud.

Table 1: Shows the time complexity for both encryption and decryption

File Size	Time Complexity	
	Existing	Proposed
1KB	255	231
5KB	330	297
10KB	350	311
15KB	390	329
20KB	620	599

As shown in Table 1, it is evident that the time complexity of existing and proposed systems is presented against different file sizes.

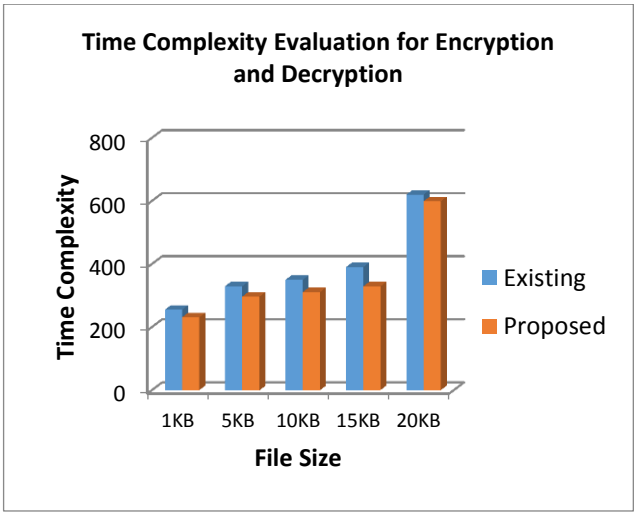

Figure 24: Time complexity evaluation for encryption and decryption

As presented in Figure 24, it is evident that the size of file is presented in horizontal axis and the time complexity is presented in vertical axis. The results revealed that the file size has its bearing on the performance in terms of time complexity. The proposed system showed better performance.

Table 2: Shows the PSNR values for quality analysis

File Size	PSNR Values	
	Existing	Proposed
1KB	4.8481	7.927
5KB	4.856	7.6878
10KB	4.8397	7.6631
15KB	4.8508	7.7519
20KB	4.8564	7.7129

As shown in Table 2, it is evident that the PSNR values of images used in existing and proposed systems are presented against different file sizes.

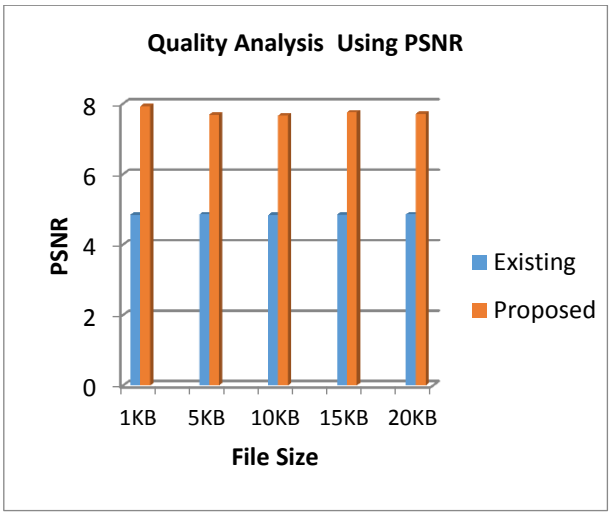

Figure 25: Quality evaluation with PSNR measure

As shown in Figure 25, it is evident that the horizontal axis presents the file sizes against which experiments are made. The vertical axis on the other hand presents PSNR values observed to estimate the quality of existing and the proposed methods. The results revealed that the file size has its impact on the PSNR values. Another important observation is that the proposed method showed better quality in terms of PSNR when compared with the existing system. From the results it is understood that he proposed system is able to reduce time complexity for encryption and decryption besides the quality of the outsourced image content.

VI. CONCLUSIONS AND FUTURE WORK

In this paper, we proposed a methodology that combines both cryptography and steganography in order to outsource a secret message to public cloud. The cloud computing has emerged to be the platform for storing and computing of data. In this context, it is important to take care of security of data to be outsourced. With respect to confidential messages that are to be kept in public cloud or that are to be transmitted without losing security, it is possible to use the proposed methodology. The methodology has two underlying algorithms known as Multi-Stage Secret Text Encryption and Embedding and Multi-Stage Secret Text Extraction and Decryption. LSB based steganography is used in the process of achieving secret message sharing. Secret message is encrypted and embedded into a cover image. It makes use of 4x4 Zig Zag scan, crossover and modified rail fence mechanism. The experimental results are evaluated with metrics like time complexity and PSNR. The results revealed that the proposed method is useful in securing and sharing secret messages or outsourcing them to public cloud. This work can be extended further to accommodate audio and video as stego media and integrate with content protection system to safeguard intellectual property of multimedia content providers.

REFERENCES

[1] M.Y. Wu, M.C. Yu, J.S. Leu, and S.K. Chen, "Improving security and privacy of images on cloud storage by histogram shifting and secret sharing," Proceedings of the 83th IEEE Vehicular Technology Conference, Nanjing China, pp. 1-5, May 2016.

[2] H. Reza, and M. Sonawane, "Enhancing mobile cloud computing security using steganography," Journal of Information Security, Vol. 7, No. 4, pp. 245-259, July 2016.

[3] J. Stone, "Reddit Fappening ban triggers outraged response from nude photo distributor," International Business Times, September 2014. (http://www.ibtimes.com/reddit-fappening-ban-triggers-outragedresponse-nude-photo-distributor-1681708)

[4] T. Gopalakrishnan, and S. Ramakrishnan, "Image encryption in blockwise with multiple chaotic maps for permutation and diffusion," ICTAT Journal on Image and Video Processing, Vol. 6, No. 3, pp. 1220-1227, February 2016.

[5] S.S. Dharwadkar, and R.M. Jogdand, "A user identity management protocol using efficient dynamic credentials," International Journal of Scientific Engineering and Research, Vol. 2, pp. 42-47, June 2014.

[6] M.G. Charate, and S.R. Bhosale, "Cloud computing security using Shamir's secret sharing algorithm from single cloud to multi cloud," International Journal of Advanced Technology in Engineering and Science, Vol. 3, pp. 349-357, April 2015.

[7] K.S. Seethalakshmi, Usha. B, Sangeetha. K. N, "Security Enhancement in Image Steganography Using Neural Networks and Visual Cryptography", IEEE Int. Conf.Computation System and Information Technology for Sustainable Solutions (CSITSS), 2016.

[8] SadafBukhari, Muhammad ShoaibArif, M.R. Anjum, and SamiaDilbar, "Enhancing security of images by Steganography and Cryptography techniques", IEEE Int. Conf. Innovative Computing Technology (INTECH), 2016.

[9] Ria Das, Indrajit Das, "Secure Data Transfer in IoT environment: adopting both Cryptography and Steganography techniques", IEEE Int. Conf. on Research in Computational Intelligence and Communication Networks (ICRCICN), 2016.

[10] AnkitGambhir and SibaramKhara, "Integrating RSA Cryptography & Audio Steganography", IEEE ICCCA, 2016.

[11] Kamaldeep Joshi, RajkumarYadav, "A New LSB-S Image Steganography Method Blend with Cryptography for Secret Communication", IEEE ICIIP, 2015.

[12] Vipul Shanna and Madhusudan "Two New Approaches for Image Steganography Using Cryptography" IEEE Int. Conf. Image Information Processing, 2015.

[13] MoreshMukhedkar, PrajktaPowar and Peter Gaikwad, "Secure non real time image encryption algorithm development using cryptography & Steganography", IEEE INDICON, 2015.

[14] RiniIndrayani, HanungAdiNugroho, RisanuriHidayat, IrfanPratama, "Increasing the Security of MP3 Steganography Using AES Encryption and MD5 Hash Function", International Conference on Science and Technology-Computer (ICST), IEEE, 2016.

[15] Nikhil Patel, ShwetaMeena, "LSB Based Image Steganography Using Dynamic Key Cryptography", International Conference on Emerging Trends in Communication Technologies (ETCT), 2016.

[16] Dan Gonzales, Jeremy M. Kaplan, Evan Saltzman, Zev Winkelman, And Dulani Woods, "Triple Security Of File System For Cloud

Computing," Ieee Transactions On Cloud Computing. 5 (3), P1-14, 2017.

[17] Mark Stieninger, Dietmar Nedbal, Werner Wetzlinger, Gerold Wagner And Michael A. Erskine, "Factors Influencing The Organizational Adoption Of Cloud Computing: A Survey Among Cloud Workers," International Journal Of Information Systems And Project Management. 6 (1), P1-19, 2018.

[18] G. Preethi And N.P.Gopalan, "Data Embedding Into Image Encryption Using The Symmetric Key For Rdh In Cloud Storage," International Journal Of Applied Engineering Research. 13, P3861-3866, 2018.

[19] C. Kaleeswari, P. Maheswari, Dr. K. Kuppusamy, Dr. Mahalakshmi Jeyabalu, "A Brief Review On Cloud Security Scenarios," Ijsrst. 4 (5), P1-6, 2018.

[20] Zheng Yan,Robert H. Deng And Vijay Varadharajan, "Cryptography And Data Security In Cloud Computing," Ieee, P1-5, 2017.

[21]Swapnil Rajesh Telrandhe And Deepak Kapgate, "Authentication Model On Cloud Computing," International Journal Of Computer Sciences And Engineering. 2 (10), P1-5, 2014.

[22] Richa Arya, "Triple Security Of File System For Cloud Computing," International Journal Of Computer Science And Engineering. 2 (3), P1-7, 2014.

Authors Profile

Konakanti Bhargavi is fellow researcher in the discipline of computer science and engineering at Jawaharlal Nehru Technological University Ananathapuramu. She completed her graduation from JNTU affiliated college and post graduation from JNTU Ananathapuramu. She is a member of AMIE, UACEE, CSTA. She published 11 national and international journals/conferences. Her areas of interest are Image Processing, Software Engineering, Cloud Computing and Information Security.

Dr. Thota Bhaskara Reddy awarded Ph.D in 2006 from Sri Krishna Devaraya University, Ananathapuramu. Presently he is working as professor in the department of computer science and Application at Sri Krishna Devaraya University, Ananathapuramu. He published about 81 national and international journals/conferences. His areas of interest are Image Processing, Cloud Computing, Computer Networks, Data Mining, and Software Engineering.

