Security Improvement of Cloud Data Using Hybrid Cryptography and Steganography

Mustafa S. Abbas
College of Information Technology
University of Babylon
Babil, Iraq
mustafasaeidd@gmail.com

Suadad S. Mahdi
College of Information Technology
University of Babylon
Babil, Iraq
suadadsafaa@gmail.com

Shahad A. Hussien
College of Information Technology
University of Babylon
Babil, Iraq
shahad.alshamare@gmail.com

***Abstract*—One of the significant advancements in information technology is Cloud computing, but the security issue of data storage is a big problem in the cloud environment. That is why a system is proposed in this paper for improving the security of cloud data using encryption, information concealment, and hashing functions. In the data encryption phase, we implemented hybrid encryption using the algorithm of AES symmetric encryption and the algorithm of RSA asymmetric encryption. Next, the encrypted data will be hidden in an image using LSB algorithm. In the data validation phase, we use the SHA hashing algorithm. Also, in our suggestion, we compress the data using the LZW algorithm before hiding it in the image. Thus, it allows hiding as much data as possible. By using information concealment technology and mixed encryption, we can achieve strong data security. In this paper, PSNR and SSIM values were calculated in addition to the graph to evaluate the image masking performance before and after applying the compression process. The results showed that PSNR values of stego-image are better for compressed data compared to data before compression.**

Keywords— Cloud Storage, Symmetric Cryptography, Asymmetric Cryptography, LZW Algorithm, Steganographic

I. Introduction

Through its services in recent years in most organizations, government departments, banks, etc., information technology has witnessed a significant revolution which is mainly attributed to cloud computing [1]. The cloud computing is categorized based on the services it provides to three layers: infrastructure as a service (IaaS), software as a service (SaaS) and platform as a service (PaaS) [2].

IaaS provides users with virtual machines and storage so they can build their infrastructure on them. Further, SaaS provides platforms to develop cloud-hosted applications for users in order to use them in building, developing, testing and managing their applications. In contrast, PaaS provides services and applications to users anytime, anywhere through a web browser. Despite the many benefits that cloud computing offers, the most important are storing, retrieving and transferring data through the cloud quickly and easily. Therefore, the problem of data security is a major challenge because data is stored at a third party and threats are greatest when users store their data in a clear form [3].

Typically, there are two techniques used to protect sensitive data: cryptography and steganography. Cryptography is defined as converting data into unreadable codes [4]. Encryption algorithm typically uses a specific parameter or key for the data conversion procedure. Some encryption algorithms require one key to encrypt and decrypt called symmetric encryption. However, other encryption algorithms need two keys: for encryption, they need a public key and a private key for decryption. Decryption is often categorized alongside encryption on the contrary—decryption results from the encrypted data of the original data.

Steganography is another technique for protecting data through hiding confidential data in a cover object such as image, voice, and text [5]. The strength of the steganography system depends on the ability to integrate and indistinctness data into the cover object. Consequently, the confidential information is not recognized or retrieved by the unauthorized user.

Digital files such as image and sound are more suitable as a cover object in steganography due to the characteristics of higher redundancy of digital files [6]. Thus, it obtains an effective way to hide data.

In this paper, a new way is proposed to protect the data stored in the cloud by combining the techniques of cryptography and steganography. This proposed method encrypts secret data in a hybrid way using the symmetric encryption algorithm AES256 and the asymmetric encryption algorithm RSA. Then, the encrypted data is compressed and sent to the LSB algorithm to be hidden. Hash functions are used without the need for a third party to confirm the impartiality of the data quickly after retrieval [7].

The performance of a steganography technique is evaluated and compared based on some criteria to check the quality of the stego-image {Formatting Citation}. In this paper, PSNR and SSIM are used, in addition to the histogram.

This paper is divided as follows: Section II highlights the relevant works. Section III tackles the proposed work; while in section IV, the outcomes of the work will be discussed. Finally, section V states the conclusions of this study.

II. Related Work

Many techniques have been suggested and implemented to protect data stored in the cloud environment. The authors in [9] had suggested a method for steganography technique consisting of two steps. The first step is the pre-processing algorithm that reduces the size of the secret images. While in the second step, they used an algorithm as an embedding mechanism that is based on the Fibonacci representation of pixel intensity. Their results showed the effectiveness of their method against the RS and steganalyser WS attacks. However, the proposed method did not achieve the confidentiality of confidential data through the use of encryption methods.

In [10], the authors proposed a hybrid model of data securely stored in the cloud-based on encryption and steganography. Where confidential data is encrypted using the AES algorithm, and then the encrypted information is hidden

978-1-7281-5249-3/20/$31.00 ©2020 IEEE

using LSB before it uploading to the cloud. While in [11], the authors used Blowfish encryption algorithm and Least Significant Bits (E-LSB) for steganography. Also, they used the SHA-256 hash algorithm to check integrity for improving cloud storage security. Their results showed that a good PSNR value was obtained to hide 1KB data as an image.

An algorithm for generating random keys using a secret public / private key pair was proposed in [12]. The process accomplished when data was encrypted by its owner using a network of a festal structure along with the public key. Then the data was embedded to image and uploaded to the cloud. In [13], the researchers suggested a system combining steganography with quantum cryptography in order to increase the confidentiality of data. The Quantum One Time Pad algorithm was used for encryption data then, hidden secret data in a cover image before sending over a quantum channel. The results showed the efficiency and effectiveness of the proposed system by calculating values of PSNR and display histogram analysis. While authors in [14] used AES encryption algorithm for encrypting their image and then indexed into the cover image via steganography. They suggested integrating a Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) to obtain the stego image. At the final stage, a stego image was uploaded for storage in the cloud.

In [15], the authors suggested encrypting data in the cloud with the AES algorithm by a secret key. Then secret encryption key uses ECC algorithm and indexes in the user's image. In this way, the problem of key management is solved. An IDEA algorithm and a Least Significant Bit Grouping (LSBG) algorithm were suggested being using to include and extract the secret information in the cover image [16]. This approach reveals a breakthrough in reducing data security problems. A system for improving the security of data storage in cloud by image steganography partition random edge-based technique is performed in [16]. For enhancing security, they divide the original image into several parts. Edge-based algorithms are applied, and random pixels are selected (pixels based on prime numbers) of each segment, and data is entered into them.

Most authors have not considered ways to reduce the size of confidential data before embedding it in the cover image, and thus affect image resolution standards if large data is embedded.

III. Proposed System

This section presents the design of a new system for providing complete security of sensitive data in the public cloud model. The public cloud has been chosen as an example of cloud types. This is because it is available to anyone who wants to use it. This means that the proposed system works with hybrid, private, or community cloud deployment models. The flowchart of the proposed system is explained in Fig. 1. The following processes are included:

- Encryption: The secret data upload to the cloud will be encrypted using a hybrid encryption system.
- Compression: Encrypted data will be compressed to reduce its size and allow more data to be hidden using steganography techniques. In this work, the Lempel-Ziv-Welch (LZW) compression algorithm was used, which proved to be effective in reducing the data size and speed, as will be shown in the results in the next section.
- Embedding: Here, we will hide data that has been compressed into a cover image using the Least Significant Bit (LSB) embedding algorithm that will create a stego-image as an output.

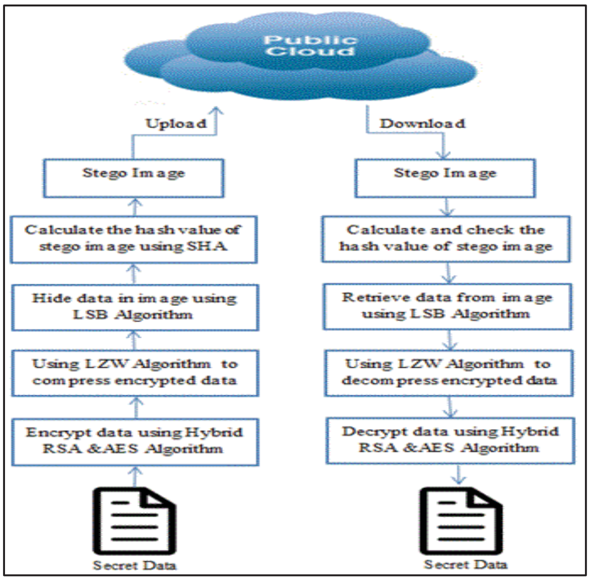
Public Cloud
Upload
Download
Stego Image
Stego Image
Calculate the hash value of stego image using SHA
Calculate and check the hash value of stego image
Hide data in image using LSB Algorithm
Retrieve data from image using LSB Algorithm
Using LZW Algorithm to compress encrypted data
Using LZW Algorithm to decompress encrypted data
Encrypt data using Hybrid RSA &AES Algorithm
Decrypt data using Hybrid RSA &AES Algorithm
Secret Data
Secret Data

Fig. 1. Diagram of Proposed Cloud Security System

In our work, hybrid encryption consists of the AES-256 and RSA algorithms, where both RSA and AES are effective algorithms used in the cloud environment [17]. The hybrid encryption depends on dividing secret data into odd and even-data based on location in the data array. Odd-data is encrypted using the AES algorithm with 256 key sizes that generate by a random number generator (RNG). The RNG generates a sequence of numbers that cannot be predicted correctly and are proved the randomize by NIST randomness tests [18]. While even-data is encrypted using RSA algorithm. Where AES key distribution used for encryption is carried out securely.

a. The key is generated by random number generators (RNGs), which are available in many computer software libraries.

b. It is encrypted using the RSA algorithm and the public key.

c. Finally, the key is sent to the second party in securely way. The hybrid encryption of the secret data is also mentioned in Algorithm I.

Algorithm I: Hybrid RSA&AES256 Encryption

```
Input:   PlainText
Output: Full_Encryption_array,  Encryption_key
Begin:
  1.Convert PlainText into binary format and store them in one-
      dimensional array
  2.Split binary array into two parts (Odd_array, Even_array)
      based on location in array
  3.Generate AES key (key) 256 bit using RNG
  4.Encryption_Odd = Encrypt_AES256 (Odd_array, key)
  5.Generate RSA key (public key= pu_key, private key=
      pr_key)
  6.Encryption_Even = RSA (Even_array,  pu_key)
  7.Full_Encrypt_array by integrate  Encryption_Odd and
      Encryption_Even
  8.Encryption_key = RSA (key, pu_key)
  9.Return Full_Encryption_array & Encryption_key
End
```

In the LSB algorithm, every bit of the data to be hidden is written to the last bit of a byte of the data that creates the cover image. In the proposal, 24-bit images were used, as three bits of information were included in each pixel, one in each layer of the RGB colours of the cover image, as explained in Fig. 2.

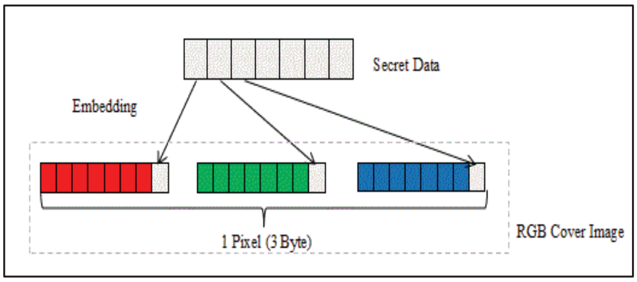

Fig. 2. Embedding Secret Data in RGB Image

In this way, it allows reducing the cloud storage used and providing protection for transferred data.

When the data owner decides to share his data with the other party, he only needs to send the stego hash value and the AES key that is encrypted. Then, the next steps are performed by the receiver to retrieve confidential data:

- Calculate Hashing: In this step, we will calculate the hash value of the stego image to confirm the data integrity when retrieved from the cloud. Moreover, integrity was implemented using the SHA-256 algorithm in this work. Then, the data owner uploads the stego image to the cloud storage.
- Checking Hash: In this step, the data integrity is checked after downloading stego-image from the cloud by calculate hashing for it and comparing the value with the stored hash value.
- Recovery: Here, the stego-image data is extracted by the receiver by applying the LSB algorithm and then extracting the merged bits from the cover image will be possible.
- Decompression: After the data is retrieved from the cover image, it is decompressed and retrieved in its original size by using the LZW algorithm.
- Decryption: In this step, the extracted data will be decrypted by the hybrid algorithm. The hybrid decryption is implementing based on Algorithm 2.

```
Algorithm II: Hybrid RSA&AES256 Decryption
Input: Full_Encryption_array, Encryption_key

Output: PlainText

Begin:
    1. Split Full_Encryption_array into two parts (Odd_array,
       Even_array) based on location in array
    2. Generate RSA key (public key= pu_key, private key=
       pr_key)
    3. key= RSA (Encryption_key, pr_key)
    4. Decryption_Odd = Decrypt_AES256 (Odd_array, key)
    5. Decryption_Even = RSA (Even_array, pr_key)
    6. Full_Decryption_array by integrate Decryption_Odd and
       Decryption_Even
    7. Convert Full_Decryption_array into PlainText format
    8. Return PlainText
End
```

IV. Experimental Results and Analysis of the Proposed System

In the present study, Python language is used to implement the proposed system and also to verify the efficiency and effectiveness of the current proposal. In general, the amount of data that can be hidden within the cover image is a critical evaluation criterion. Using the proposed system, the data size can be minimized by using the data compression algorithm. It is thereby increasing the data size that can be hidden in a cover image.

For evaluating the proposed system's performance, several RGB images are used as cover images and hide a message containing a different number of characters in each cover image. Then, the evaluation is performed through the calculation of the signal-to-noise ratio (PSNR) as a parameter. "(1)" is used to calculate the value of PSNR, but first, the value of Mean Square Error (MSE) is needed to be calculated according to "(2)". The structural similarity index (SSIM) matrix of the stego-image is also calculated using "(3)" where SSIM refers to the symmetry between the cover image and the misleading image of the information steganography technology.

$$PSNR = 10\log_{10}\frac{C_{\max}^{2}}{MSE} \qquad (1)$$

Where $C_{\max}$ indicates the maximum value holds in the image.

$$\mathrm{MSE} = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}(C-S)^{2} \qquad (2)$$

Where C is the cover image, and S is the stego-image. m, n are number of rows and columns of the cover image and the stego-image.

$$\mathbf{SSIM}\,(\mathbf{x},\mathbf{y}) = (2\mu_x\mu_y + c_1)(2v_{xy} + c_2)\Big/(\mu_x^2 + \mu_y^2 + c_1)(v_x^2 + v_y^2 + c_2)$$

(3)

Where μ is average values of x, y. V_x and V_y are the standard deviation, and V_{xy} is the cross-covariance for the image. A secret message with size 1KB is hidden in each of the cover images. The result of the PSNR value analysis for each stego-image before and after compression, as shown in Table I.

TABLE I. Comparison of PSNR Values for Stego-Image

Cover Image	PSNR (dB)	
	Without compression	With compression
Lena.png	69.769	71.580
Baboon.png	69.890	71.750
Peppers.png	70.057	72.211
Cat.png	71.249	73.476
Average PSNR	70.241	72.254

The results show that the PSNR values for RGB stego-images of the proposed system with data compression have better performance for all the tested images. This shows the difficulty of noticing the difference between the cover image and stego-image. In other words, the higher the PSNR value, the harder it becomes for visual attackers to recognize the stego-image. The second measurement to measure stego-image quality is SSIM. The result shows a similarity between the cover image and the stego-image where the SSIM value is closer to 1 (SSIM for all images tested is 0.999), which means that the stego-image is of outstanding quality.

Figure 3 shows the cover image histogram and the stego-image, and the results show that the histogram is similar when observed with the naked eye. This entails that the amount of distortion of the stego-image is very small. The last stage of evaluation of the proposed system is figuring the time for both the process of hybrid encryption, steganography and compression as well as the calculation of the total time. The results show that the time taken is very little for the system proposed, which reflects the efficiency of the proposed system, as shown in TABLE II.

TABLE II. PROPOSED SYSTEM PERFORMANCE

Size	**Response Time (in seconds)**			
	Encryption	*Compression*	*Steganography*	*Full-Time*
1KB	0.14	0.01	0.09	0.24
2KB	0.16	0.03	0.09	0.28
4KB	0.20	0.07	0.10	0.37
8KB	0.31	0.10	0.12	0.53
15KB	0.40	0.12	0.15	0.67

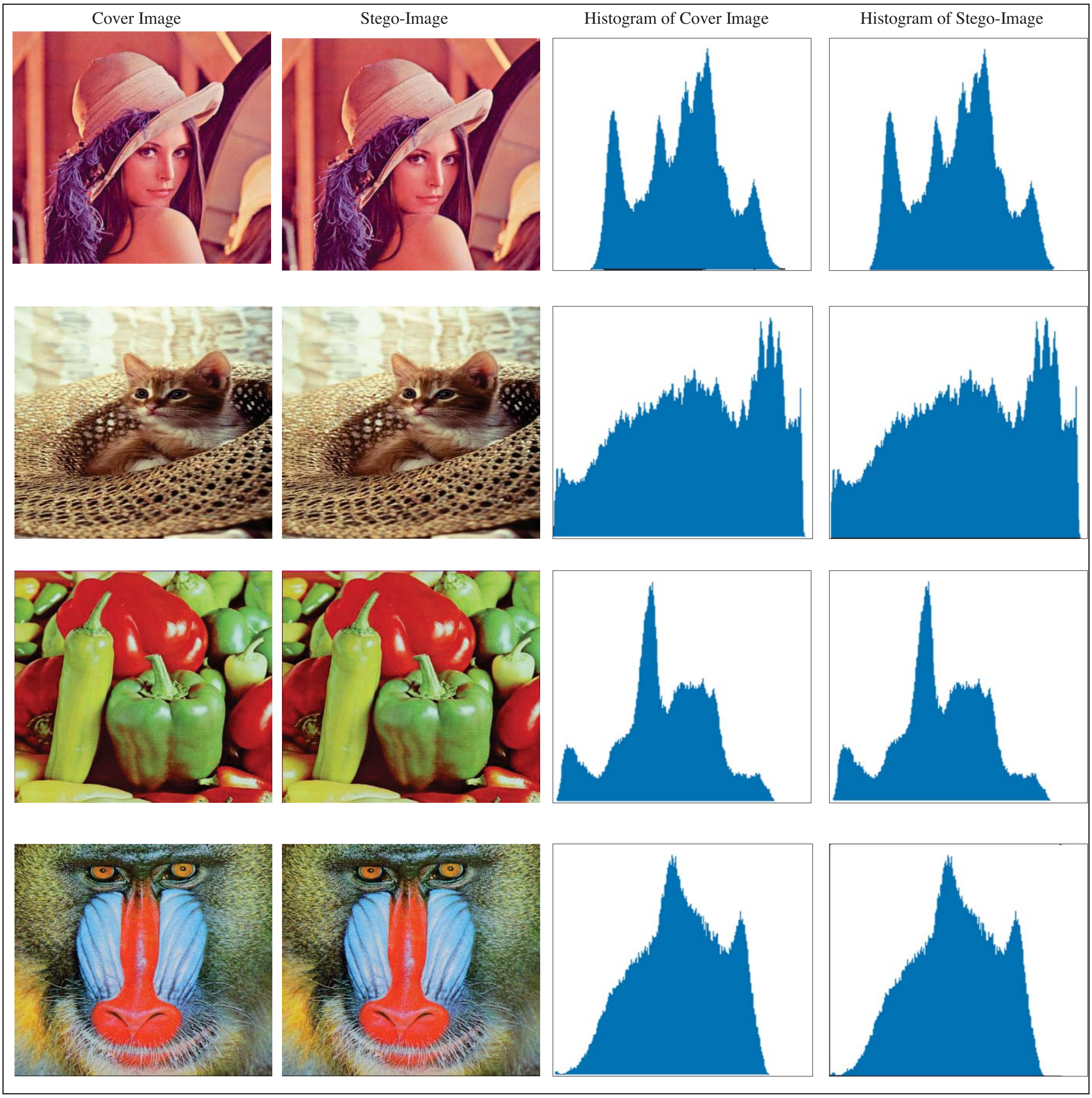

Fig. 3. Histogram of stego-image

V. Conclusions

This study successfully combined two of the security techniques: cryptography and steganography to provide double security for stored data in the cloud environment. We have presented hybrid encryption where symmetric algorithm AES combine with asymmetric algorithm RSA is used to secure stored data in the cloud. The results of the encryption of secret data are then hidden in the image using the LSB algorithm after encrypted compression data. In this proposal, the amount of data hidden in the image increases while the distortion on the image is reduced compared to the results of data concealment without compression using the LSB algorithm.

This system is more powerful and efficient for securing the data in the cloud environment. Besides, it is more powerful to verify the integrity of data after retrieval from the cloud. Therefore, it can be said in this paper that security objectives have been achieved. The experimental results showed that the stego-image quality after hiding 1 KB data with the average PSNR value of 72.254 for all tested image.

References

[1] S. E. Elgazzar, A. A. Saleh, and H. M. El-Bakry, “Overview of using private cloud model with GIS,” Int. J. Electron. Inf. Eng., vol. 7, no. 2, pp. 68–78, 2017.

[2] E. F. Coutinho, F. R. de Carvalho Sousa, P. A. L. Rego, D. G. Gomes, and J. N. de Souza, “Elasticity in cloud computing: a survey,” Ann. Telecommun. des télécommunications, vol. 70, no. 7–8, pp. 289–309, 2015.

[3] S. C. Sukumaran and M. Misbahuddin, “DNA Cryptography for Secure Data Storage in Cloud.,” IJ Netw. Secur., vol. 20, no. 3, pp. 447–454, 2018.

[4] S. William, Computer security: Principles and practice. Pearson Education India, 2008.

[5] L.-C. Huang, L.-Y. Tseng, and M.-S. Hwang, “A reversible data hiding method by histogram shifting in high quality medical images,” J. Syst. Softw., vol. 86, no. 3, pp. 716–727, 2013.

[6] R. Shanthakumari and S. Malliga, “Dual-layer security of image steganography based on IDEA and LSBG algorithm in the cloud environment,” Sādhanā, vol. 44, no. 5, p. 119, 2019.

[7] Y. Zhang, C. Xu, H. Li, and X. Liang, “Cryptographic public verification of data integrity for cloud storage systems,” IEEE Cloud Comput., vol. 3, no. 5, pp. 44–52, 2016.

[8] A. A. Abdulla, “Exploiting similarities between secret and cover images for improved embedding efficiency and security in digital steganography.” University of Buckingham, 2015.

[9] A. A. Abdulla, H. Sellahewa, and S. A. Jassim, “Stego quality enhancement by message size reduction and Fibonacci bit-plane mapping,” in International Conference on Research in Security Standardisation, 2014, pp. 151–166.

[10] N. Garg and K. Kaur, “Hybrid information security model for cloud storage systems using hybrid data security scheme,” Int. Res. J. Eng. Technol., vol. 3, no. 4, pp. 2194–2196, 2016.

[11] M. O. Rahman, M. K. Hossen, M. G. Morsad, and A. Chandra, “An Approach for Enhancing Security of Cloud Data using Cryptography and Steganography with E-LSB Encoding,” IJCSNS, vol. 18, no. 9, p. 85, 2018.

[12] S. Shanthi, R. J. Kannan, and S. Santhi, “Efficient secure system of data in the cloud using steganography based cryptosystem with FSN,” Mater. Today Proc., vol. 5, no. 1, pp. 1967–1973, 2018.

[13] A. A. Abdullah, Z. A. Abod, and M. S. Abbas, “An Improvement Steganography System Based on Quantum One Time Pad Encryption,” Int. J. Pure Appl. Math., vol. 119, no. 15, pp. 263–280, 2018.

[14] G. S. Mahmood, D. J. Huang, and B. A. Jaleel, “Achieving an Effective, Confidentiality and Integrity of Data in Cloud Computing.,” IJ Netw. Secur., vol. 21, no. 2, pp. 326–332, 2019.

[15] O. Hosam and M. H. Ahmad, “Hybrid design for cloud data security using combination of AES, ECC and LSB steganography,” Int. J. Comput. Sci. Eng., vol. 19, no. 2, pp. 153–161, 2019.

[16] D. Suneetha and R. K. Kumar, “Enhancement of Security for Cloud Data Using Partition-Based Steganography,” in Proceedings of the 2nd International Conference on Data Engineering and Communication Technology, 2019, pp. 201–209.

[17] P. Semwal and M. K. Sharma, “Comparative study of different cryptographic algorithms for data security in cloud computing,” in 2017 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA)(Fall), 2017, pp. 1–7.

[18] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker, “A statistical test suite for random and pseudorandom number generators for cryptographic applications,” Booz-Allen and Hamilton Inc Mclean Va, 2001.