

An Improvement for Cloud Data Security Model Using Image Steganography

Afrah Albalawi^{1†} and Nermin Hamza^{2††},

¹ Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia

² Faculty of Graduate Studies for Statistical Research, Cairo University, Cairo, Egypt

Summary

Nowadays, cloud computing is used by individuals and organizations to store their data. In the cloud storage, a third party manages the data which is a drawback of this service since the data is vulnerable. Consequently, a model that will protect the data stored in the cloud is needed. This paper proposed a hybrid model using encryption and image steganography to protect data from unauthorized access. The proposed model uses hash function, RSA encryption algorithm, AES-256 encryption algorithm, compression and LSB steganography algorithm. The proposed model is evaluated using many experiments and compared with other existing model. The results show that the proposed model satisfies the three objectives of image steganography: quality; where the proposed model produces a stego image with high quality; more than 40 dB, security; where the secret data is difficult to detect and capacity, where the proposed model allows to hide large amounts of data.

Keywords:

Security; image steganography; cryptography; cloud storage; information security.

1. Introduction

According to the United States National Institute of Standards and Technology (NIST) cloud computing is defined as "A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [1]. Cloud computing also can be defined as a large amount of resources pooled together, to be shared by users [2]. It allows users to share IT resources and pay depending on use, it enables expansion when required [3], easy to share and transfer data [4].

Organizations and individuals have commonly used cloud storage as one of the cloud services to store their data in the cloud [5]. Instead of building data centers, users need only to apply for storage services to the storage service provider [6]. In cloud storage, data can be accessed anytime and everywhere, and storage spaces are large [7].

Some of stored data may be sensitive, that made the cloud storage service providers a target of attackers [5].

Confidential data needs to be secured against internal and external threats [6]. Usually, cryptography and steganography are used to protect cloud data [7]. In the cryptography, the data will be encrypted then uploaded to the cloud [8]. But the data still exists as a secret data after encryption. It could be decrypted by an attacker if he has enough time [6]. In steganography, the existence of the secret data is hidden, where the confidential data is embedded within a cover media such as text, video and image [7].

Due to the popularity of images on the internet, the image steganography is the most used steganography [9]. Image steganography is embedding secret data within a cover image. The image steganography uses two domains to hide data: transform domain and spatial domain [10]. The spatial domain covers secret data by manipulating the actual carrier values, but the transform domain obtains the transmission coefficients by taking the values to a different domain [11].

This paper proposes a model to protect cloud data against unauthorized access. This model use hash function, encryption, compression and image steganography. This paper is structured as follows: section 2 provides an overview of some basic concepts. Section III presents a literature review of basic concepts and recent works. Section IV displays the proposed model. In section V, the evaluation and comparisons are presented. Section VI concludes the paper.

2. Background

2.1 Cloud Computing

This subsection describes the cloud computing characteristics, the cloud computing models and the cloud computing service models.

2.1.1 Cloud Computing Characteristics

Cloud computing is exciting for IT applications and services because of its characteristics. The characteristics of the cloud computing are displayed below:

- **On-demand self-service:** Services are allocated automatically on demand [12].
- **Cost effectiveness:** The payment in the cloud computing depends on pay as per usage. Furthermore, there is no infrastructure that needs to be maintained, this leads to decrease costs [12].
- **Mobility:** The service is accessible by any device everywhere and anytime [12].
- **Rapid elasticity:** When required, the service is provided quickly and elastically [12].
- **Multitenancy:** Many users can share the service at the same time [12].
- **Scalability:** Easy to modify the infrastructure, such as add or remove nodes or servers [12].
- **Customization:** It is possible to customize the service and infrastructure based on user demand, where the cloud computing is a reconfigurable environment [12].
- **Efficient resource utilization:** The use of on-demand services makes it possible to use resources efficiently [12].
- **Measured services:** The ability to monitor, control, and report on cloud services provides transparency for both the provider and the customer [13].

2.1.2 Cloud Computing Models

According to NIST definition the cloud computing deployment models have four types:

- **Public cloud:** The cloud service provider provides the service for the public. The service is managed by the provider [12].
- **Private cloud:** The service provided for a single organization, and the service managed by the organization [12].
- **Community cloud:** the cloud service provider provides a service for many organizations [12].
- **Hybrid cloud:** It is a combination of two or more models, such as public and private cloud [14].

2.1.3 Cloud Computing Service Models

- **Software as a service (SaaS):** A service is provided for users on demand. The service can be accessed and used from a web interface [2].
- **Platform as a service (PaaS):** A platform is provided by cloud service providers for users to develop their applications or websites [2].

- **Infrastructure as a service (IaaS):** Cloud service providers provide infrastructure to users [2].
- **File storage as a service (FSaaS):** Cloud providers provides users with the ability to store, manage and access data from an interface of the browser. The cloud provider holds the responsibility of maintenance and oversees the storage infrastructure [7].

2.2 Steganography

A review of the steganography system, steganography types, image steganography objectives and some of the popular image steganography techniques are presented in this subsection.

2.2.1 Steganography System Components:

- **Cover object:** A media file used to conceal secret data[15].
- **Stego media:** The file produced from hiding secret data within a cover object [15].
- **Secret data:** The data to be hidden within a cover object [15].
- **Steganalysis:** Process of detecting the existence of secret data [15].

2.2.2 Steganography types

- **Text steganography:** A text file is used as a cover object to hide secret data [16].
- **Audio steganography:** It describes the process of using a sound file as a cover object to embed secret data [16].
- **Image steganography:** When an image is used as a cover object to embed secret data, it is set to be an image steganography [16].
- **Video steganography:** This type of steganography uses a video file to conceal secret data [17].

2.2.3 Image steganography objectives

The efficiency of an image steganography technique is evaluated based on the following objectives:

- **Visual quality:** The quality of a produced stego image must be similar to the original image quality [18].
- **Capacity:** It refers to the maximum number of secret data bits can be embedded within a cover image [18].

- **Security:** The secret data cannot be detected by an attacker [19]. If the existence of hidden data is able to be proved, the technique is considered to be insecure [20].

The ideal technique must satisfy these three objectives simultaneously. But most often, steganographic techniques that have high payload capacity produce stego images with high distortion which make it vulnerable to steganalysis. Moreover, steganographic techniques produce stego images with high quality suffer from the low payload. Due to the contradictions between them, how to achieve the three objectives is a big challenge [21].

2.2.4 Image steganography techniques

The embedding process is the backbone of the steganographic system. Data can be hidden in the cover image over spatial domain or transform domain. The most popular techniques of image steganography are presented in the following:

- **Least Significant Bit (LSB):** Uses the least significant bit of cover image pixels to embed secret data bits. A stego image produced using this technique has similar characteristics of the original image [22].
- **Discrete Wavelet Transform (DWT):** This approach converts the object into a wavelet domain, then processes the coefficients and performs the inverse of the transform [22].
- **Discrete Cosine Transform (DCT):** Converts the cover image into frequency domain; high, middle, and low frequency. A secret data embedded in the middle frequency where the changes will not affect the original image's visibility [23].

3. Literature Review

Many models have been proposed for protecting data stored in the cloud. This section provides an overview of some recent models used image steganography to protect the data stored in the cloud.

To address the problem of unauthorized access to data stored in the cloud, Amalarethinam and FathimaMary [24] proposed a model by using a combination of obfuscation and steganography. This model uses the Magical Rolling Alpha Digits Obfuscation (MRADO) to convert secret data to obfuscated format. Then, the obfuscated data will be embedded within a cover image using LSB steganography technique. As a result of the experiments, the randomness of MRADO square contributes to enhance the security;

where even if the attacker extracts the data hidden in an image, he still requires the de-obfuscation technique to decipher the data. The proposed technique enhances the quality of stego image. The authors did not report the payload capacity of the proposed model.

Ebrahim et al. [25] used steganography and encryption to prevent unauthorized access to cloud data. The proposed model consists of three phases. The first phase, uses SHA-256 to calculate the hash value of data file, then the calculated hash value and the session key are encrypted using RSA encryption. The second phase, the secret data is encrypted using AES-256 encryption. The third phase, hides the encrypted data in a cover image using advanced LSB steganography algorithm. The proposed model was evaluated and compared to other models. The proposed model provides protection against cryptanalysis attacks, steganalysis, and statistical changes and it has a high payload capacity. However, when hiding a large amount of data, producing a stego image with low quality.

To enhance the security of cloud data, Rahman et al. [26] proposed a new model using cryptography, steganography, and hash function. The proposed model consists of three steps. First, encryption; where the Blowfish algorithm is used to encrypt secret data. Second, embedding; the encrypted data is embedded within a cover image using Embedded Least Significant Bit (E-LSB) algorithm. Third, hashing; use SHA-256 to compute hash value of stego image. To evaluate the proposed model, the authors tested different types of attacks. The outcome of the experiments shows that the hidden data cannot be detected by detection attacks (such as RS attack and virtual attack), but this model is sensitive to destruction attacks (such as format conversion, JPEG compression and salt&pepper).

Kumar and Suneetha [27] presented a new model to enhance the security, decrease the performance time of embedding and extracting process, and increase the quality of a produced stego image. In this model, a cover image is divided into three color components. These components will be processed to obtain the shuffled position, which will be used to generate three random private keys. The AES algorithm is used to encrypt secret data. Then, use the generated random keys to embed the encrypted data in color components. The final step is embedding the color components in one image to produce a stego image. The authors evaluated the proposed model using various size of images and different secret data sizes. The outcomes of the experiments shows, this model produces a stego image with good quality, but it has a low payload capacity.

To increase security of data transfer over cloud Garg et al. [28] introduced a new technique using split algorithm, encryption and steganography. In this technique, initially, the secret data is encrypted using AES algorithm. Then, use LSB steganography algorithm to embed the encrypted data within a cover image. Finally, the produced stego image will be splitted into n parts, these parts will be stored or transformed over the cloud. The authors did not evaluate quality and capacity of the proposed technique.

To improve the cloud data security, Abbas et al. [29] presented a new model using encryption, steganography, and hash function. For the encryption, the message is stored in a binary array, then split the array into odd and even arrays. The odd array is encrypted using AES-256 encryption, and the even array is encrypted using RSA encryption. Then, embed the concatenation of the arrays into a cover image using LSB. The authors suggested compressing the data using LZW compression to increase the number of data bits can be embedded within a cover image. The result of the experiments proves that the proposed model produces a stego image with good quality, but it does not allow to hide large amount of data.

In 2020, Astuti et al. [30] proposed a model to improve the security of data on the cloud by using a combination of encryption and steganography. This model consists of two steps. First, use AES-128 algorithm to encrypt the data. Second, embed the encrypted data into a cover image using the LSB steganography algorithm. The authors evaluated their work by embedding different size of text data files in JPG/JPEG images. The proposed model allows to hide large amounts of data, but it increases the load on memory.

From the literature, it could be noticed that all the reviewed models provide security for the cloud data, but the models having high payload capacity produce a stego image with low quality, and the models having good image quality suffer from low payload capacity.

4. Proposed Model

To enhance the security of data stored in the cloud, this paper proposes a hybrid model using a combination of cryptography and steganography. The proposed model uses many algorithms. The SHA-256 function is used to ensure the data integrity. Also, RSA and AES-256 encryption algorithms are used to protect the confidentiality. To decrease the size of secret data the compression is used. Finally, the LSB steganography algorithm is used to embed the secret data within a cover image.

The proposed model consists of two phases. Embedding phase, is the process of embedding secret data within a cover image. Extracting phase, is the process of retrieving data from a stego image. Fig. 1 summarizes the embedding and extracting processes.

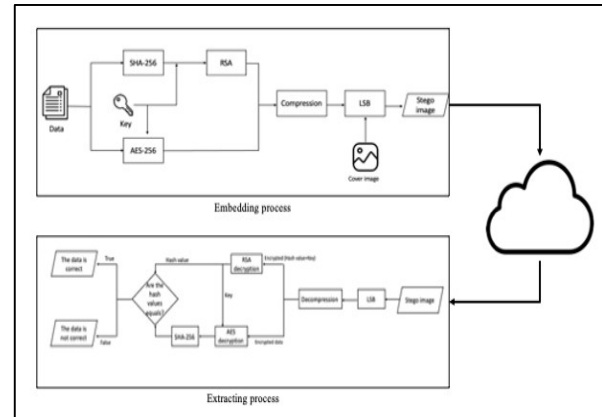


Fig. 1 The proposed model processes

In the embedding phase, a text data is embedded in an RGB image by applying the following steps:

1. Compute the hash value of secret data using SHA-256.
2. Generate a key using a random key generation.
3. Encrypt secret data using AES-256 with the generated key.
4. The computed hash value and the generated key are combined, then encrypted using RSA encryption with a public key. The public and private keys are generated using (ESRKGS) proposed by Thangavelet al. [31].
5. Combine the two encrypted data (RSA output + AES output), then compress the combined file using GZIP compression.
6. The compressed data will be hidden in RGB image using LSB algorithm proposed in [32], and produce a stego image.
7. The produced stego image will be uploaded to the cloud.

In the extracting phase, the secret data will be extracted from a stego image by following these steps:

1. Download a stego image from the cloud.
2. Apply the inverse of the LSB algorithm to extract data from the image.

3. The extracted data will be decompressed using GZIPdecompression.
4. Split the decompressed data into two parts; encryptedkey and hash value, and encrypted data.
5. Decrypt the encryption of (hash value + key) usingRSA decryption with a private key.
6. The extracted key is used with AES decryption to decrypt the secret data.
7. Compute the hash value of the decrypted data using SHA-256.
8. Compare the computed hash value with the extracted hash value to ensure the integrity, if they are equal that means the extracted data is correct, otherwise thedata is not correct.

5. Evaluation and Experiments

The proposed model was implemented in MATLAB released R2020a, and it is evaluated based on the three objectives of image steganography: security, quality and capacity. In order to evaluate and measure these objectives and obtain the advantages and limitations of the proposed model, the following measurementsare used:

- **Histogram analysis:** The histogram analysis is used to evaluate the security. It displays a graph whose x-axis and y-axis represents the difference of pixel between each pair and the number of occurrences, respectively. To identify the pixels distribution or monitor unusual shapes as a result of an embedding algorithm, compare the histogram of cover image and the histogram of stego image [17]. If there are undesiredsteps in the histogram, that means steganography is detected [33].
- **Mean Square Error (MSE):** This metric is used to evaluate the quality of the images. It is the average of the difference between the original image and the stego image [34]. The MSE calculation is defined asin Eq. 1:

$$MSE = \frac{1}{mn} \sum_{i=1}^m \sum_{j=1}^n (Y_{ij} - \hat{Y}_{ij}) \quad (1)$$

Where m is the number of rows in the images and n is the number of columns in the images. Y_{ij} and \hat{Y}_{ij} refer to pixel value from the cover image and stego image, respectively.

- **Peak signal-to-noise Ratio (PSNR):** It measures the similarity between the cover image and the

stego image [35]. Eq. 2 is used to calculate the PSNR.

$$PSNR = 10 \log_{10} \left(\frac{255^2}{MSE} \right) \quad (2)$$

If the PSNR value is more than 40 dB it is set be of a very good quality. In other word, the distortion is very low. If it is in between 30 dB and 40 dB, it setto be acceptable, however, a PSNR value less than 30 dB that means the distortion is very high [33].

- **Maximum hiding capacity:** It refers to the maximum number of data bits that can be embedded within a cover image. It can be expressed as bits or bytes or kilobytes [33].
- **Bit rate:** It is the maximum amount of data bits that can be embedded per pixel, it is referred as bits per pixel (bpp) or bits per byte(bpb) [33]. Bits per pixel are determined by Eq. 3

$$bpp = \frac{\text{Embedding capacity}}{W \times H} \quad (3)$$

Where W represents the width of the cover image and H represents the height of the cover image.

Table 1 provides the results of hiding different text files of various sizes within the airplane image of 512x512 pixel size.

From Table 1, the stego image quality is different basedon the amount of embedded data. It can be noticed that the smaller amount of hidden data produces a stego image with higher PSNR value. In fact, in the proposed model when hideslarge data the computed PSNR value is above 40dB. In other words, the distortion in stego image is undetectable.

Fig. 2 represents the relation between embedded data size and the PSNR value. It can be observed that there is an inverse relation between the size of hidden data andthe quality of the produced stego image; an increased the embedded data would inevitably result in a decreased quality.

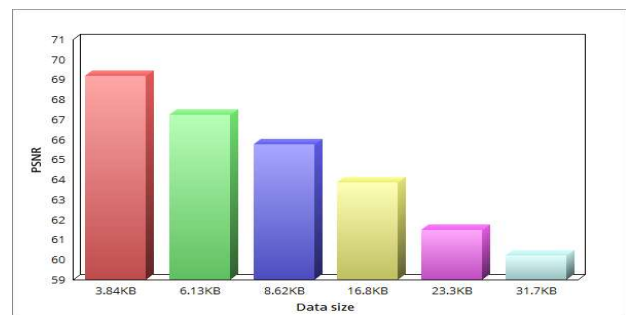







Fig. 2. The relation between the data size and the PSNR value

Table 2 shows a comparison of the PSNR results of the proposed model with regards to the compression (with and without) to evaluate the performance. The comparison is done by embedding different amounts of data in the airplane image of size 512x512.

Table 1: Results of study the impact of data size

<i>Stego image</i>	<i>Data size (KB)</i>	<i>PSNR (dB)</i>
	3.84	69.1754
	6.13	67.2255
	8.62	65.7629
	16.8	63.8374
	23.3	61.5024


	31.7	60.1869
--	------	---------

Table 2: Results of the proposed model with compression and without compression

<i>Data size (KB)</i>	<i>PSNR</i>	
	<i>With compression</i>	<i>Without compression</i>
3.84	69.0981	66.4990
8.62	65.8199	63.5662
11.6	64.5340	62.3458

From the Table 2, it can be concluded, the use of compression reduced the amounts of the embedded data, which increased the quality of the produced stego images, where the increasing of the quality is 3.5%. The results from Table 2 are represented in Fig. 3.

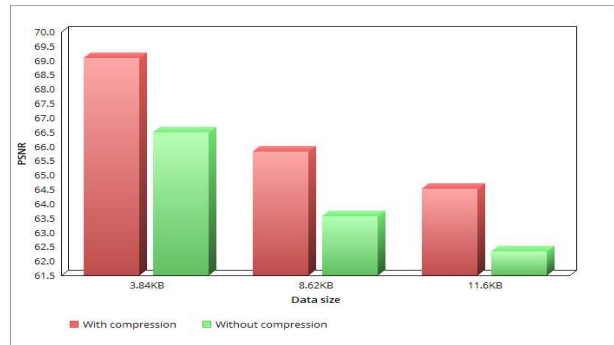
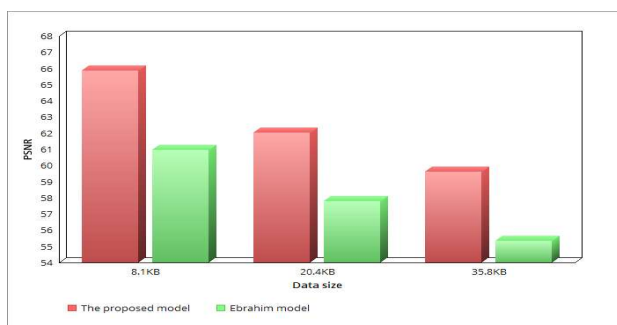


Fig. 3 Comparison of the proposed model with compression and without compression.

Finally, the proposed model was compared with Ebrahim model proposed in [25]. The comparison is done by hiding various amounts of data in the Baboon image. Table 3 shows the PSNR values of the proposed model and Ebrahim model. The results show that the proposed model had higher PSNR values than the other model. The results are illustrated in Fig. 4.

Table 3: Comparison of the proposed model and Ebrahim model

Data size (KB)	PSNR	
	Proposed model	Ebrahim model
8.1	65.8817	60.9636
20.4	62.0378	57.8107
35.8	59.6192	55.3391

**Fig. 4** Comparison of the proposed model and Ebrahim model

6. Conclusion

Data stored in the cloud faces several security issues. One of the effective solutions used for protecting data in the cloud is the image steganography. In image steganography, the existence of secret data is concealed by embedding it into a cover image. This paper proposed a hybrid model to secure data stored in the cloud. The proposed model uses hash function, encryption algorithms, compression and steganography algorithm. The proposed model was evaluated by many experiments and compared with other existing models. The results show that the proposed model provides security for data, allows to hide large amounts of data and produces a stego image with high quality.

References

- [1] Singh, S., Sharma, P. K., Moon, S. Y., Park, J. H.: Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions. In: *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–18 (2017).
- [2] Sharma, Y., Gupta, H., Khatri, S. K.: A security model for the enhancement of data privacy in cloud computing. In: *2019 Amity International Conference on Artificial Intelligence (AICAI)*. IEEE, pp. 898–902 (2019).
- [3] Renuka, S., Kumar, N. S.: A survey on cloud data security. In: *International Journal of Computer Sciences and Engineering*, vol. 7, no. 4, pp. 88–95 (2019).
- [4] Markandey, A., Dhamdhere, P., Gajmal, Y.: Data access security in cloud computing: A review. In: *2018 International Conference on Computing, Power and Communication Technologies (GUCON)*. IEEE, pp. 633–63 (2018).
- [5] Sood, S. K.: A combined approach to ensure data security in cloud computing. In: *Journal of Network and Computer Applications*, vol. 35, no. 6, pp. 1831–1838 (2012).
- [6] Datta, B., Bandyopadhyay, S. K.: Cloud steganography—a review. In: *Journal for Research— Volume*, vol. 2, no. 01, (2016).
- [7] AlKhamese, A. Y., Shabana, W. R., Hanafy, I. M.: Data security in cloud computing using steganography: a review. In: *2019 International Conference on Innovative Trends in Computer Engineering (ITCE)*. IEEE, pp. 549–558 (2019).
- [8] Wang, R.: Research on data security technology based on cloud storage. In: *Procedia engineering*, vol. 174, pp. 1340–1355 (2017).
- [9] Hamid, N., Yahya, A., Ahmad, R. B., Al-Qershi, O. M.: Image steganography techniques: an overview. In: *International Journal of Computer Science and Security (IJCSS)*, vol. 6, no. 3, pp. 168–187 (2012).
- [10] Mustafa, G., Ashraf, R., Haq, I. U., Khalid, Y., Islam, R. U.: A review of combined effect of cryptography & steganography techniques to secure the information. In: *2019 5th International Conference on Computing Engineering and Design (ICCED)*. IEEE, pp. 1–6 (2019).
- [11] Sharafi, J., Khedmati, Y., Shabani, M. M.: Image steganography based on a new hybrid chaos map and discrete transforms. In: *Optik*, vol. 226, p. 165492 (2021).
- [12] Rashid, A., Chaturvedi, A.: Cloud computing characteristics and services: a brief review. In: *International Journal of Computer Sciences and Engineering*, vol. 7, no. 2, pp. 421–426 (2019).
- [13] Vinoth, S., Vemula, H. L., Haralayya, B., Mamgain, P., Hasan, M. F., Naved, M.: Application of cloud computing in banking and e-commerce and related security threats. In: *Materials Today: Proceedings 51*: 2172-2175 (2022).
- [14] Alhenaki, L., Alwatban, A., Alamri, B., Alarifi, N.: A survey on the security of cloud computing. In: *2nd International Conference on Computer Applications Information Security (ICCAIS)*, pp. 1–7 (2019).
- [15] Choudry, K. N., Wanjari, A.: A survey paper on video steganography. In: *International Journal of Computer Science and Information Technologies*, vol. 6, no. 3, pp. 2335–2338 (2015).
- [16] Rakhi, S. G.: A review on steganography methods. In: *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, vol. 2, no. 10 (2013).
- [17] Hashim, M., MOHDRAHIM, M. S., ALWAN, A. A.: A review and open issues of multifarious image steganography techniques in spatial domain. In: *Journal of Theoretical & Applied Information Technology*, vol. 96, no. 4 (2018).

- [18] Ahmad, M. A., Elloumi, M., Samak, A. H., Al-Sharafi, A. M., Alqazzaz, A., Kaid, M. A., Iliopoulos, C. : Hiding patients' medical reports using an enhanced wavelet steganography algorithm in DICOM images. In: Alexandria Engineering Journal 61.12 10577-10592 (2022).
- [19] Albalawi, A., Hamza, N.: A survey on cloud data security using image steganography. In: International Journal of Advanced Computer Science and Applications, vol. 11, 01 (2020).
- [20] Chandramouli, R., Kharrazi, M., Memon, N. : Image steganography and steganalysis: Concepts and practice. In: International Workshop on Digital Watermarking. Springer, pp. 35–49 (2003).
- [21] Hussain, M., Wahab, A. W. A., Idris, Y. I. B., Ho, A. T., Jung, K. H. : Image steganography in spatial domain: A survey. In: Signal Processing: Image Communication, vol. 65, pp. 46–66 (2018).
- [22] Tiwari, A., Yadav, S. R., Mittal, N. K. : A review on different image steganography techniques. In: International Journal of Engineering and Innovative Technology (IJEIT), vol. 3, no. 7, pp. 121–124 (2014).
- [23] Goel, S., Rana, A., Kaur, M. : A review of comparison techniques of image steganography. In: Global Journal of Computer Science and Technology (2013).
- [24] Mary, B. F., Amalarethinam, D. G.: Data security enhancement in public cloud storage using data obfuscation and steganography. In: 2017 World Congress on Computing and Communication Technologies (WCCCT). IEEE, pp. 181–184 (2017).
- [25] Ebrahim, M. A., El-Maddah, I. A., Mohamed, H. K. "Hybrid model for cloud data security using steganography. In: 2017 12th International Conference on Computer Engineering and Systems (ICCES). IEEE, pp. 135–140 (2017).
- [26] Rahman, M. O., Hossen, M. K., Morsad, M. G., & Chandra, A.: An approach for enhancing security of cloud data using cryptography and steganography with e-lsb encoding. In: *IJCSNS*, vol. 18, no. 9, p. 85 (2018).
- [27] Kumar, R. K., Sunetha, D. : A secure steganography approach for cloud data using ann along with private key embedding. In: International Journal of Computer Science and Information Security (IJSIS), vol. 16, no. 6 (2018).
- [28] Garg, P., Sharma, M., Agrawal, S., & Kumar, Y. : Security on cloud computing using split algorithm along with cryptography and steganography. In: International Conference on Innovative Computing and Communications. Springer, pp. 71–79 (2019).
- [29] Abbas, M. S., Mahdi, S. S., Hussien, S. A. : Security improvement of cloud data using hybrid cryptography and steganography. In: 2020 International Conference on Computer Science and Software Engineering (CSASE). IEEE, pp. 123–127 (2020).
- [30] Rawat, D., Bhandari, V. :Steganography technique for hiding text information in color image using improved lsb method. In: International Journal of Computer Applications, vol. 67, no. 1, (2013).
- [31] Thangavel, M., Varalakshmi, P., Murrall, M., Nithya, K.: An enhanced and secured rsa key generation scheme (esrks). In: Journal of information security and applications, vol. 20, pp. 3–10, (2015).
- [32] Astuti, N. R. D. P., Aribowo, E., Saputra, E. : Data security improvements on cloud computing using cryptography and steganography. In: IOP Conference Series: Materials Science and Engineering, vol. 821, no. 1. IOP Publishing, p. 012041 (2020).
- [33] Pradhan, A., Sahu, A. K., Swain, G., Sekhar, K. R. : Performance evaluation parameters of image steganography techniques. In: 2016 International Conference on Research Advances in Integrated Navigation Systems (RAINS), pp. 1–8, (2016).
- [34] Gutub, A., Al-Shaarani, F. : Efficient implementation of multi-image secret hiding based on lsb and dwt steganography comparisons. In: Arabian Journal for Science and Engineering, pp. 1–14 (2020).
- [35] Almohammad, A., Ghinea, G. : Stego image quality and the reliability of psnr. In: 2010 2nd International Conference on Image Processing Theory, Tools and Applications, pp. 215–220 (2010).