A Survey on Cloud Data Security using Image Steganography

Afrah Albalawi[1], Nermin Hamza[2]
Faculty of Computing and Information Technology, King Abdulaziz University
Jeddah, Saudi Arabia[1,2]
Faculty of Graduate Studies for Statistical Research, Cairo University[2]

***Abstract*—Now-a-days, cloud computing proved its importance where it is being used by small and big organizations. The importance of cloud computing is due to the various services provided by the cloud. One of these services is storage as a service (SaaS) which allows users to store their data in the cloud databases. The drawback of this service is the security challenge since a third party manages the data. The users need to feel safe to store their data in the cloud. Consequently, we need for models that will enhance the data security. The image steganography is a way to protect data from unauthorized access. Image steganography allows users to conceal secret data in a cover image. In this paper, we review and compare some of the recent works proposed to protect cloud data using image steganography. The first comparison of models based on the algorithms they used, advantages and drawbacks. The second comparison of the models based on the aims of steganography: quality where the model produces a stego-image with high quality, security where the secret data is difficult to detect and capacity where the model allows to hide large amounts of data.**

Keywords*—*Security; cloud computing; image steganography; data hiding; data storage

I. Introduction

Cloud computing provides flexible services for users by combining many of resources and applications based on a pay-as-you-need concept [1]. One of the services provided by the cloud is store data in the cloud. This service provides fast distribution, low-cost and reliability [2].

When storing data in cloud storage, storage devices has vulnerability to internal leakage, hacking and other reasons that may lead to lose data confidentiality [3].

Some of data stored in the cloud are very sensitive data, such as banking and government information, which must be protected against unauthorized people including the cloud service provider [2].

There are many researches that use cryptography techniques to protect the cloud confidentiality of the data [1], but the main disadvantage of encryption is although the data is encrypted and became unreadable, it is still exists as a secret data. The attacker could decrypt the data if he has enough time [4]. Steganography is a way to solve this problem since it allows the user to hide data into other object such as text, image, audio or video, these techniques will increase the sensitive data security [1]. In this paper, we focus on the image steganography to protect cloud data. Fig. 1 illustrate the usage of image steganography in cloud environment.

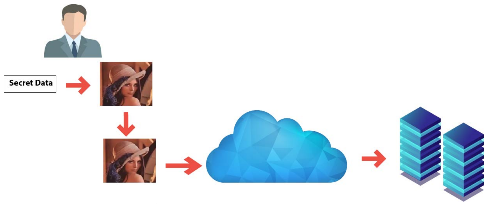

Fig. 1. The usage of image steganography in cloud environment

In this paper, we check the existing cloud data security techniques used image steganography. This paper is structured as follows. Section II, present an overview of cloud computing. Section III, give an overview of steganography. In Section IV, we introduce an overview of image steganography. In Section V, we review some of recent techniques of cloud data security using image steganography. In Section VI, we compare the techniques based on different aspects and discuss the current status. In Section VII, we discuss the future works.

II. Cloud Computing Overview

In this section, we give an overview of the cloud computing, service models, deployment models and security requirements of cloud computing.

Cloud computing provides IT services to users over the Internet. The NIST defined cloud computing as “a model for enabling ubiquitous, convenient, on-demand network access to 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 and or service interaction” [5].

A. *Service Model of Cloud Computing*

- Software as a service (SaaS): User can only use the applications provided by the provider without ability to manage the applications [6].
- Platform as a service (PaaS): User creates applications on the cloud infrastructure and the user will be able to deploy and manage the applications [6].
- Infrastructure as a service (IaaS): User will provide the fundamental computing resources, such as networks, storage and processing [6].
- File storage as a service (FSaaS): The cloud provides the ability to store, manage and access the data from

an interface of browser. the cloud provider holds the maintenance responsibility and oversees the infrastructure storage [7].

B. Deployment Model of Cloud Computing

- Private cloud: Cloud service provider makes the resources and applications available to cloud users. The users must subscribe to get the benefits of the resources, and they will pay based on the subscription [6].
- Public cloud: Users use the resources dynamically over the Internet, and they will pay based on their use [6].
- Hybrid cloud: It consists of distributed private clouds linked together and have a central management. The payment system in this model is complex [6].

C. Cloud Computing Security Requirements

- Audit: It includes authentications and authorisation, to ensure user's identity by implementing a strong verification process [8].
- Confidentiality: Protect data stored in the database from unauthorized users [8].
- Integrity: It is used to ensure the data consistency, and to protect data from iteration [9].

III. Steganography Overview

In this section, we presents an overview of the steganography, its types, its objectives.

Steganography is the science of hiding the secret data in a multimedia file [10]. Steganography as a word is combine of two Greek words "Sregano" and "Graphy", and the meaning is "cover writing" [11].

A. Types of Steganography

- Text steganography: Use text file to hide secret data [12].
- Image steganography: Hide secret data in a cover image [13].
- Audio steganography: Use an audio file to conceal secret data [13].
- Video steganography: Hide secret data in a video file [14].
- DNA-based steganography: Employ randomness of DNA to embed secret data [15].
- Protocol steganography: Hide secret data in network protocol such as, IP, TCP and UDP [16].

B. Objectives of Steganography

- Security: The attacker unable to detect the secret data [7].
- Payload (Capacity): Allow to hide large amount of data into the cover object [7].
- Invisibility (Quality): The changes in the cover object undetectable by the Human Visual System (HVS) [7].

IV. Image Steganography Overview

This section, provides an overview of image steganography, some techniques of image steganography and types of images.

The image steganography is the process of hiding the secret data in a cover image to produce a stego image [7].

A. Some of Image Steganography Techniques:

- Least Significant Bit (LSB) based Steganography: Hide the bits of secret data in the LSB of the cover image. This technique is the most popular used [17].
- Discrete Cosine Transform (DCT): Use subdivision of quantized DCT coefficient to hide the secret data [17].
- Discrete Wavelet Transform (DWT): It is used to decompress the image mathematically into a set of wavelet [7]. This technique used for medical and military applications [17].

B. Types of Images

- The binary images: consists of black and white pixels [7].
- The grayscale images: consists of pixels with shades of gray colors [7].
- The color images: uses some integration of red, green and blue to specify the pixels' colors [7].

V. Current Works Proposed for Cloud Data Security using Image Steganography

In this section, we review some works proposed for cloud data security using image steganography.

Mohis and Devipriya in [2], proposed an improved approach that increases the security of public cloud data by using mediated certificateless public key encryption (MCL-PKE) and LSB steganography algorithm. The proposed system consists of three modules: registration module, cloud module and embedding module. In the registration module, the user registers to the cloud and generates public and private keys, keep the private key for the users and transfer the public key to the Key Generation Centre (KGC). In the cloud module, if the user requests the data the Security Mediator (SEM) check if the user legitimate it will decrypt partially the data and will provide it to the user, then the user fully decrypts it using the private key. In the embedding module, the user before storing the data in the cloud he will embed the sensitive data within an image. The authors compared the proposed approach with other system. The proposed approach reduces overhead at the owner side, and reduces unauthorized access on the data. This technique does not produce high quality stego image and does not allow to hide large amount of data.

Ebrahim et al. [1] combined encryption and steganography to prevent unauthorized access to cloud data. In the proposed model, there are three phases. The first phase, compute hash value of secret data using SHA-256, then use RSA to encrypt the hash value and session key. The second phase, use AES-256 to encrypt the secret data. The third phase, use advanced LSB algorithm to hide encrypted data in a cover image. The authors were evaluated the proposed model and compared it with other models. The result shows this model provides security against cryptanalysis and steganalysis attacks and stetisstical changes, and produces a stego image with high quality.

Seshubhavan et al. in [18], used steganography and genetic algorithms to secure the data in the cloud. The proposed technique tries to insert the secret data in suitable pixels in the cover image without affecting the characteristics of the cover image. This technique work only on the grayscale image. Therefore, if the cover image is colored image convert it to gray scale image, then extract the least significant bit and most significant bit and convert them to 0's and 1's array. Use the AES algorithm to encrypt the secret data and the key converted to 0's and 1's array. The two arrays combined and split into R Block, and L Block. These segments are applying to genetic algorithm to produce an address block, which is used to embed the secret data in the cover image and produce the stego image that will store in the cloud database. This algorithm compared with other existing algorithms. The result shows that, the proposed algorithm is better quality, but does not provide high capacity payload.

Rahman et al. [19] proposed a new combination of encryption and steganography to secure cloud data. They used blowfish algorithm to encrypt secret data, to embed encrypted data in a cover image E-LSB algorithm is used, and to preserve the integrity of produced stego image they used SHA-256. The analysis of the proposed model presents the model provides security against statistical and visual attacks.

Suneetha and Kumar in [20] have improved the security of cloud data by using partition random edge-based technique for image steganography. They supposed this technique will help to reduce changes between cover image and produced a stego image. In the embedding process, convert the cover image into grayscale image and portion it into 9 partitions. Then, use Canny edge detection method to identify the edge pixels and select the prime number of random pixels of an image. After that encrypt the secret data and embed the key in the selected pixels. The authors compared their method with others existing methods and the result shows that, this method is better and works on different types of data. It provides security against steganalysis attack. This work focuses on security and quality, but ignores the amount of data can be embedded in the cover image.

Kumar and Suneetha [21] used image segmentation along with image steganography to increase the security of data in cloud environment. To embed secret data in a cover image covert the cover image into black and white or grayscale image, then apply the image segmentation technique to identify and extract the iris part of the cover image. After that use Canny edge detection to select edge pixels of inner and outer circle, and use RSA algorithm to encrypt the secret data. Hide the secret key in the selected pixels and store the stego image in the cloud. The authors were analyzed the technique and the result shows that this technique provides better security than others existing techniques based on steganography and segmentation.

Shanthakumari and Malliga [22] proposed a combination of International Data Encryption Standard Algorithm (IDEA) and Least Significant Bit Grouping (LSBG) algorithm to improve security and capacity of data embedding to the cover image. In the embedding phase, the IDEA algorithm performed to encrypt secret data, then LSBG is applying to embed the encrypted data into cover image and produce stego image which is uploaded to the cloud. In the extracting phase, download the stego image from the cloud and use LSBG to extract the secret data, then perform IDEA decryption to decrypt the secret data. The authors were evaluated the proposed technique and compared it with other techniques. The result shows this technique provides good security for secret data and produces stego image with high quality and increase the embedding capacity.

VI. Discussion

In this section, we compare the current techniques based on different aspects and discuss the current status.

Table I shows a comparison of the reviewed techniques based on the algorithms they used, advantages and drawbacks. From Table I, we conclude there is no technique totally strong without weaknesses, each technique has its own strengths and weaknesses.

In Table II, we compare the current techniques based on steganography objectives: security, capacity and quality.

From Table II, we can conclude all proposed techniques satisfies the security objective, and five of them produces a stego image with high quality, but only one technique allows to hide large amounts of data.

The reviewed techniques works on different types of images where [18] and [20] suitable for a grayscale image, [21] works on black and white or grayscale images and some suitable for color image such as [1], [19] and [22].

VII. Future Work

for the future work, we intend to improve efficient solutions that satisfy the objectives of steganography. These solutions should allow to hide large amounts of data, produce a stego image with high quality and the hidden data must be undetectable.

VIII. Conclusion

Cloud computing provides many benefits to the users but it has security challenges. Image steganography is a way to protect secret data in the cloud by hide the secret data in a cover image. This paper, present a review of some

TABLE I. COMPARING CLOUD DATA SECURITY ALGORITHM USED IMAGE STEGANOGRAPHY

Author	Algorithms used	Advantages	Drawbacks
[2]	-Mediated certificateledd public key encryption (MCL-PKE). -LSB steganography.	-Reduce overhead at the owner side. -Protect the secret data against unautherized access.	-Does not produce a stego image with high quality. -Does not allow to hide large amount of data. -Expensive and difficult. -Does not provide how to instant revocation when desired.
[1]	- SHA-256 - RSA encryption algorithm - AES-256 encryption algorithm advanced LSB steganography algorithm.	- Allows to embed any type of data in any format of image. - Produces stego image with high quality. - Protects cloud data against attacks and statistical changes.	- Capacity of embedded data depends on the size of cover image. - Time consuming.
[18]	-Genetic algorithm. -AES encryption algorithm.	Allows to insert secret data in cover image without affecting the characteristic of the cover image.	-use only with gray scale images.
[19]	- Blowfish encryption algorithm - E-LSB steganography algorithm - SHA-256	Provides security against statistical and visual attacks.	Ignores the quality of stego image and capacity of embedded data.
[20]	-Partition random edge-based. -Canny edge detection. -Encryption algorithm.	-Reduces changes between cover image and stego image produced. -Suitable for different type of data. -Provide security against steganalysis attach.	-Used only for grayscale images. -Time consuming. -High requirements on memory.
[21]	-Image segmentation. -Canny edge detection. -RSA encryption algorithm.	increase the security.	-Using for black and white or grayscale images. -Time consuming. -High requirements on memory.
[22]	-IDEA encryption technique. -LSBG steganography algorithm.	- Increase the security. - Produce stego image with high quality - Allow to hide large amount of data.	IDEA uses large number of weak keys.

TABLE II. COMPARING THE TECHNIQUES BASED ON STEGANOGRAPHY OBJECTIVES

Author	*Security*	*Quality*	*Capacity*
[2]	Yes	No	No
[1]	Yes	Yes	No
[18]	Yes	Yes	No
[19]	Yes	No	No
[20]	Yes	Yes	No
[21]	Yes	Yes	No
[22]	Yes	Yes	Yes

recently proposed techniques for cloud data security using image steganography. We compared these techniques based on algorithms they used, advantages and drawbacks, and based on the objectives of steganography. We concluded each technique has its own advantages and weaknesses which make it difficult to choose one technique as the best solution.

References

[1] M. A. Ebrahim, I. A. El-Maddah, and H. K. Mohamed, "Hybrid model for cloud data security using steganography," in *2017 12th International Conference on Computer Engineering and Systems (ICCES)*. IEEE, 2017, pp. 135–140.

[2] M. Mohis and V. Devipriya, "An improved approach for enhancing public cloud data security through steganographic technique," in *2016 International Conference on Inventive Computation Technologies (ICICT)*, vol. 3. IEEE, 2016, pp. 1–5.

[3] R. Wang, "Research on data security technology based on cloud storage," *Procedia engineering*, vol. 174, pp. 1340–1355, 2017.

[4] B. Datta and S. K. Bandyopadhyay, "Cloud steganography-a review," *Journal for Research— Volume*, vol. 2, no. 01, 2016.

[5] P. R. Kumar, P. H. Raj, and P. Jelciana, "Exploring data security issues and solutions in cloud computing," *Procedia Computer Science*, vol. 125, pp. 691–697, 2018.

[6] G. Ramachandra, M. Iftikhar, and F. A. Khan, "A comprehensive survey on security in cloud computing," *Procedia Computer Science*, vol. 110, pp. 465–472, 2017.

[7] A. Y. AlKhamese, W. R. Shabana, and I. M. Hanafy, "Data security in cloud computing using steganography: A review," in *2019 International Conference on Innovative Trends in Computer Engineering (ITCE)*. IEEE, 2019, pp. 549–558.

[8] M. Yesilyurt and Y. Yalman, "New approach for ensuring cloud computing security: using data hiding methods," *Sādhanā*, vol. 41, no. 11, pp. 1289–1298, 2016.

[9] Y. AlHumaidan, L. AlAjmi, M. Aljamea, and M. Mahmud, "Analysis of cloud computing security in perspective of saudi arabia," in *2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom)*. IEEE, 2018, pp. 1–4.

[10] A. S. Ansari, M. S. Mohammadi, and M. T. Parvez, "A comparative study of recent steganography techniques for multiple image formats," *International Journal of Computer Network and Information Security*, vol. 11, no. 1, p. 11, 2019.

[11] I. J. Kadhim, P. Premaratne, P. J. Vial, and B. Halloran, "Comprehensive survey of image steganography: Techniques, evaluations, and trends in future research," *Neurocomputing*, vol. 335, pp. 299–326, 2019.

[12] A. Beroual and I. F. Al-Shaikhli, "A review of steganographic methods and techniques," *International Journal on Perceptive and Cognitive Computing*, vol. 4, no. 1, pp. 1–6, 2018.

[13] A. Arya and S. Soni, "A literature review on various recent steganography techniques," *International Journal on Future Revolution in Computer Science& Communication Engineering*, vol. 4, pp. 143–149, 2018.

[14] M. HASHIM, M. RAHIM, M. SHAFRY, and A. A. ALWAN, "A review and open issues of multifarious image steganography techniques in spatial domain." *Journal of Theoretical & Applied Information Technology*, vol. 96, no. 4, 2018.

[15] M. Hussain, A. W. A. Wahab, Y. I. B. Idris, A. T. Ho, and K.-H. Jung, "Image steganography in spatial domain: A survey," *Signal Processing: Image Communication*, vol. 65, pp. 46–66, 2018.

[16] W. A. Awadh, A. S. Hashim, and A. K. Hamoud, "A review of various steganography techniques in cloud computing," *University of Thi-Qar Journal of Science*, vol. 7, no. 1, pp. 113–119, 2019.

[17] S. Jeevitha and N. Amutha Prabha, "A comprehensive review on steganographic techniques and implementation," *ARPN Journal of Engineering and Applied Sciences*, vol. 13, p. 17, 2018.

[18] M. Seshubhavan, D. Suneetha, and S. A. Varma, "A novel approach for data security for cloud data using image steganography and genetic algorithms." *Grenze International Journal of Engineering & Technology (GIJET)*, vol. 4, no. 3, p. 137, 2018. [Online]. Available: http://search.ebscohost.com/login.aspx?direct=true&db=edb&AN=134178986&lang=ar&site=eds-live

[19] 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.

[20] 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*. Springer, 2019, pp. 201–209.

[21] R. K. Kumar and D. Suneetha, "A novel approach for data security in cloud environment using image segmentation and image steganography," in *Information Systems Design and Intelligent Applications*. Springer, 2019, pp. 75–82.

[22] 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.