Journal of Education and Science (ISSN 1812-125X)

www.edusj.mosuljournals.com

Cloud Data Storage Confidentiality Using Steganography and Visual Cryptography: A Review

Asmaa Y. Albakri[(1,2)*], **Oğuz Karan** [(1)]

[(1)]Altinbas University, Software Engineering, Information Technologies, Istanbul, Turkey [(2)] Department of Computer Science, College of Computer Science and Mathematics, University of Mosul, Mosul, Iraq

Article information

Article history:
Received: May 31, 2023
Accepted: August 14, 2023
Available online: December 01, 2023

Keywords:
Visual cryptography
Cloud computing
Steganography

Correspondence:
Asmaa Y. Albakri
213721732@ogr.altinbas.edu.tr

Abstract

Cloud computing security has emerged as one of the most significant trends in the information technology (IT) sector, and it is currently widely used in that sector, particularly with the growth of information in the cloud. The security of data stored in the cloud, and when it is transferred between users and servers, is very important. secure communication and data transfer can be achieved through the use of steganography and visual cryptography. It is one of the most important technologies for securing data and authenticating it so that only the sender and the receiver can be aware of the hidden information as well as transmitting it. In contrast, visual cryptography is a cryptographic technology that encrypts data. By having these two different branches, it is difficult for an attacker to compromise the data's confidentiality. The purpose of this paper is to review several steganography and visual cryptography that have been proposed to improve cloud security and make it more secure against cyberattacks and eavesdropping. The primary goal of this study is to investigate the capabilities of secured data, which are frequently employed by researchers. Additionally, each secured data domain's advantages and disadvantages are investigated. In order to strengthen the security mechanisms, this research concludes that visual cryptography approaches could be combined with steganography and cloud computing in the secured data realm.

DOI: 10.33899/edusj.2023.140697.1370, ©Authors, 2023, College of Education for Pure Science, University of Mosul.

1. Introduction

Since most hackers monitor and attack the network to obtain data, the Internet is no longer safe for confidential data transfer [1]. Cloud data can be exposed to danger when it is transmitted over the internet. The system is affected by viruses and malware in various ways, so this intrusion may cause the system to lose data again, so security has become the most important thing for people since hacking developed [2].

Users can update the data stored in the cloud frequently. Users can delete, insert, modify, and so forth through this interface. Nowadays, cloud computing is very popular for storing software and databases [3]. Since the software is available in the cloud, users are also able to access it and use it as a data storage facility without installing any software on their systems [4].

Amazon Elastic Compute Cloud (Amazon EC2) is a cloud computing service that supports virtual information technology (virtual IT) and lets users rent virtual computer resources [5]. In the Amazon Web Services (AWS) Cloud, Amazon EC2 provides scalable computing capacity. Google App Engine, another cloud computing service, hosts applications. Other examples of Software as a Service are Google Apps and Microsoft Office Online, Apple iCloud is used for network storage, and Digital Ocean is used for servers, which serve both as infrastructure and platform as a service[6].

There are three types of cloud computing services: A-Software as a Service (SaaS), B-Platform as a Service (PaaS), and C-Infrastructure as a Service (IaaS) [7].

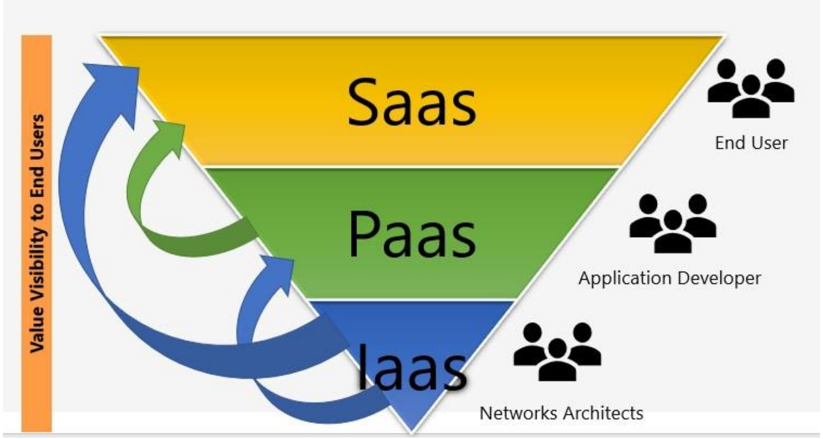

Figure 1. Structure of cloud computing

Software as a service SaaS is a layer of cloud-based software that runs as a service. Applications can also be accessed via the Internet, allowing users to work on them. In addition to SaaS, service providers can prepare applications that can be rented from the Internet through SaaS processes. The majority of companies use and provide these services. As for common use cases: SaaS is a comfortable service model for highly interoperable applications (used by multiple users internally and externally) and for short-term projects. SaaS models are preferred by small and medium-sized businesses that do not wish to invest heavily in IT maintenance. such as Google G-Suite, Dropbox, Cisco Webex, Concur, Microsoft O365, Genesys, and PayPal [8].

Most developers can build various applications with this PaaS layer, without worrying about infrastructure [9]. It also includes a range of computers and storage functions within a virtual platform delivered over the Internet and services from providers. As for, Common Use Cases: PaaS is extremely scalable and available, enabling businesses to establish new services and solutions without the need for in-house software maintenance specialists with specialized skills. IT prefers PaaS in scenarios with cloud environments such as Salesforce, AWS Elastic Beanstalk, Heroku, Google App Engine (GAE), and OpenShift[10].

As the top service layer in the cloud computing architecture, IaaS provides storage, applications, operating systems, information, data, and some network requirements for connecting cloud services [11]. A storage resource and hardware are required for IaaS. As for, Common Use Cases: Because IaaS is the cloud computing service model with the most flexibility, it is particularly useful for startups and businesses seeking agile scaling. Businesses that want more control over their resources also favor it. Such as Rackspace, Digital Ocean, Google Compute Engine, and some deployments of Microsoft Azure and Amazon Web Services (AWS) [12].

There are four types of cloud computing deployment approaches: public, private, community, and hybrid. There is more physical security in the private cloud [13]. Due to its specific internal exposure, the public cloud is more secure. The organization is even the only way to access its applications [14].

In a hybrid cloud, two or more of the above are integrated. In addition to providing additional resources, this layer provides high security [15]. Community clouds are used by other organizations that share their cloud infrastructure with customers with similar interests, such as policy requirements and security concerns [16].

The human visual system (HVS) performs the decryption of visual cryptography, introduced by Naor and Shamir in 1995. Using a visual cryptographic computation, any text or image can be fed as input and encrypted to generate an 'n' number, which is then converted into an output image (called a share). There is a lot of noise in the share. For decryption, minimum shares must be received [16].

Johannes Trithemius used the term Steganography for the first time in 1499 in his Steganographic, a treatise on cryptography and Steganography. Steganography had been accelerated by the World Wars due to the introduction of a new carrier[17].

However, when data is transferred through the cloud, security is one of the most important factors. In most cases, data is stolen during the mail transmission process, and this is due to inadequate data security. The latest technologies for protecting important data include visual cryptography and steganography. Even though they are different technologies, steganography, and visual cryptography are often confused. The important aspect is the security of the data when it is transferred through the cloud. A lack of data security usually results in data being stolen during the mail transmission process. The latest technologies for protecting data include visual cryptography and steganography. It is common for people to confuse steganography with visual cryptography, even though they are two very different technologies[18]. Using steganography and visual cryptography techniques, we examine how cloud-stored data can be made more secure against cyber-attacks.

1.1. Motivation of the Study

1-The significance of securing data is the motivation behind this study.

2-The main motive behind the use of cloud computing is to share, hide, and encrypt confidential data so that it is difficult for a hacker to discover the existence of confidential data within the object that has been shared in the cloud.

1.2. Contributions of the Study

The proposed research contributes to reviewing the modern technologies used in the field of visual cryptography and steganography and their participation in the cloud, knowing the algorithms used in this field, knowing the problems of the technologies, how they were solved, and their advantages and disadvantages.

2. Cloud Data

2.1. The Cloud Data Concept

Cloud computing results from the combination of traditional computer technology and network technology, such as grid computing, distributed computing, parallel computing, utility computing, and virtualization. One of the fundamental concepts of cloud computing is reducing the processing load on the user's terminals by perpetually enhancing the cloud's handling capacity. In the future, user terminals will be reduced to basic input and output devices. Users can utilize the powerful computing and processing capabilities of clouds, and they can order cloud services based on their specific requirements [19].

2.2. Cloud Data Architecture

Cloud storage is a system that provides data storage and business access, among other functions. Utilizing application software based on the functions of cluster applications, grid techniques, distributed file systems, etc., it assembles a large number of distinct categories of storage devices. Cloud storage can be understood merely as the storage component of cloud computing, or as a cloud computing system with a large storage capacity. The main components of a cloud storage system's architecture are the storage layer, the fundamental management layer, the application interface layer, and the access layer [19].

2.3. Cloud Data Security Issue

To effectively benefit from this new computer paradigm, increased security dangers must be overcome. The following is a list of security issues for discussion[20] :

1) Control over physical security is lost when using the cloud model since other businesses are allowed to share computing resources. no control or knowledge of the resource's location.
2) The Company has broken the law (there is a chance that a foreign government would seize data).
3) If a customer wishes to switch from one cloud provider to another, their storage services may not be compatible (for example, Google Cloud and Microsoft Cloud are incompatible).
4) Who manages the encryption and decryption keys? It makes sense that the client would be responsible.
5) Ensuring the integrity of the data (transmission, storage, and retrieval) essentially means that it only modifies in response to permitted transactions. There isn't yet a widely accepted standard to guarantee data integrity.

6) Security managers and regulators must get data logs in cases involving the Payment Card Industry Data Security Standard (PCI DSS).
7) Users must update applications to stay safe.

8) Some government rules limit what data can be held and for how long, and some bank regulators demand that client financial data stay in their home country.
9) Virtual machines' fluidity makes security consistency and record auditability challenging.
10) Cloud service companies may lose their reputation if their customers sue for privacy violations. When personal information is requested without explanation, concerns arise.

3. Relevant Reviews

3.1. The Previous Studies on Cloud Data Storage Confidentiality Using Steganography

Cloud data security has been the subject of many research works in the literature. A review of the most recent steganographic and visual cryptography techniques used to secure information in the cloud is presented in this study. In El-Latif et al.[21] described an algorithm that embeds sensitive data in the host media without pre-encrypting the data. The approach is primarily based on the embedding and security procedures that are associated with quantum walks. This technique makes use of either grayscale or colored images as a covert object to hide within the carrier image. This object could be any kind of data, such as an audio file or a text document. Additionally, the features of QWs were utilized in order to give three different kinds of image steganography that are utilized in the cloud. Quantum Walks were utilized so that the process of hiding confidential data within the host media could be controlled. The safety of the mechanism that has been described is contingent not only on the quantum behavior of quantum walks but also on the keystream that is produced by the execution of quantum walks. During the extraction process, we are going to require both the stego image and the initial key parameters. These are the settings that determine how the operating QWs on a circuit are controlled.

In their study, Singh et al. [22], hid information by employing a method known as the least significant bit, which resulted in the mobile cloud computing application being robust, dynamic, and less susceptible to image misrepresentation. In addition, they used 24-bit images, which offer the possibility of 16,000k distinct combinations and can readily hide data in a way that makes it difficult to distinguish between the changed image and the original image or the actual image. This made it difficult to determine which of the three was the genuine image. Encryption-based methods are utilized because they give a higher level of security; however, this increases the burden on the processor, which results in a decrease in performance. In order to find a solution to this problem, we turned to the idea of a key. Using an algorithm that calculates the bytes of the site where the key exists, the key is now encased in an image along with the real data or information. This process takes place after the bytes of the location where the key resides have been calculated. After installing this software, the user will only need to remember the key in order to engage in successful and secure communication.

3.2. The Previous Studies on Cloud Data Storage Confidentiality Using Visual Cryptography

Mamta et al. [23], developed an algorithm based on the concept of generating secret information shares using visual cryptography. To determine our criticality, we assign a high critical index to our data and divide it by the maximum number of shares, and assign a low critical index to our data if it is less critical. A genetic algorithm is used to encrypt and secure the shares generated in the second step. Finally, the encrypted file should be stored in the cloud and shared with an authorized user. On the server side, using a genetic algorithm, the user can download the encrypted shares from the cloud, decrypt them, and then combine the decrypted shares to form confidential data.

In Mandal and Mahmood [24], approach that utilizes both the (AES) and the Full Homomorphic Encryption (FHE) method is primarily emphasized. The authors of this study decided not to use a single type of cryptosystem to protect cloud storage, but rather a combination of different types of cryptographic protocols. They believe that if (AES) can encrypt data using a 256-bit square in only 14 cycles, then the technology might also be used for cloud computing. A fully homomorphic encryption method is used in the process of encrypting the data during the second phase. The multiplication of holomorphs results in two outcomes: the production of additional substance and multiple holomorphs. The user will only have access to the computations necessary for the chemicals that they have actually added. The user is currently making use of both the previously agreed upon secret as well as the ciphertext gained from the initial scrambling. The homomorphic material encryption method will now be utilized to mix the cipher text with the secret key. When the user employs this method, they are able to preserve the consistency, confidentiality, and secrecy of their data from any intruders.

3.3. The Previous Studies on Cloud Data Storage Confidentiality Using Visual Cryptography and Steganography

Ali and Smaiel [25], introduced a method in addition to using visual cryptography and steganography. In this method, columns and rows are replaced according to the key value, then the image is split into a group of blocks by exchanging the columns and rows for each block. In order to split the resulting image into two parts vertically, divide it into four sections and substitute between them. Shares are formed with the first part, followed by the second. During the process of forming shares, the rows of the first part are divided, then the rows of the second part, so the rows are distributed row by row. The key length must also be equal to the number of shares produced. After the share is created, the key is used to hide pixels in the two least significant bits for each share. For retrieving the hidden image from the sender, we need to know the key the sender is using to obtain the least significant bit values for the pixels in the received image and composition shares based on that key. Four sections of the image are produced, and the locations of the sections are reversed. The images are split into blocks and the columns and rows of each block are transposition separately. After obtaining the original image, the columns and rows are changed according to the key.

The data is encrypted with either the XOR or One Time Pad (OTP) algorithm as indicated by Rangaswamaiah et al. [26]. The OTP algorithm generates a random key, while the XOR algorithm uses a key input from the user. XOR can have a length that is either the same or different from the key. However, the length of the key must be the same in OTP. Cover images must be preprocessed before cipher text can be hidden. The resulting matrix consists of four sub-bands LL, LH, HL, and HH based on the LWT of the cover image. We use the LH subband to hide the data. The algorithm scrambles the pixel locations by using the scrambling algorithm. It is then followed by visual cryptography. Based on a threshold value, the Stego image is divided into two shares, and it is transferred to the receiving end. At the receiver end the same threshold level should be added and the reverse scrambling is done. The secret message is then decrypted. If the threshold value used is unknown, it is impossible to detect the secret message.

Using AES-256 and RSA together, Abbas et al. [27], established a hybrid encryption algorithm that is effective in a cloud-based environment. Based on the location of the confidential data in the data array, we divide it into odd and even groups. AES encrypts odd data with a key size of 256 using the AES algorithm. A random number generator (RNG) generates it. Using randomness tests from the National Institute of Standards and Technology (NIST), this generates random numbers. The AES key is distributed securely by encrypting the even data with the RSA algorithm. Following that, A secure method of sending the key to the second party is then used. A cover image is then created by writing each bit of data to the last bit of a byte of the data that forms the Steganography algorithm. Three bits of information were included in each pixel of the RGB cover image when 24-bit images were used.

Rosalina and Hadisukmana [28], introduced a technique that encrypts a message by using the MD5 algorithm. This technique encrypts an image by using RGB shuffle, then includes the encrypting information in a video, audio, or image by using the Least Significant Bit (LSB) technology. During the encryption phase, the researchers used the MD5 algorithm, which divides 512-bit messages into 32-bit subblocks composed of 16 pieces each. By using this method, four 32-bit blocks of data are hashed together to produce a hash value. The image is encoded using RGB shuffling. Each pixel of the image is altered depending on the input password of the user, by using the principle of RGB shuffling. Adding RGB elements with ASCII passwords and their inversions and shuffling them is the most basic way to shuffle RGB. Least Significant Bit (LSB) is the method used in steganography. The bit in the rightmost position should be changed at the beginning. By replacing bits in the confidential data with bits in the non-significant data, bits in the carrier are not as influential. The encoded data is first converted into its binary form, with one LSB for each RGB element in the image.

In addition, Shanthakumari and Malliga[29], proposed a method based on steganography and cryptography for the transmission of confidential data in a cloud environment. First, cryptography describes the execution of IDEA to encrypt the secret information as a text or file to achieve a high level of security. Second, the LSBG algorithm and gray code procedure are used to embed the encrypted data in image pixels to secure the secret information within the cover medium, thereby adding a single additional layer of security. Ultimately, the primary objective of dual-layer protection is attained by combining techniques in the field of data transmission. IDEA and LSBG provide two-tiered protection for a secure data transmission process over an optimal communication channel, which is divided into two phases. The first phase encrypts and embeds the payload in the cover medium, while the second phase defines the extraction and decryption of secret data.

Further, Mondal et al. [30], developed a technology that inserts text into the cover image. When the values of R, G, and B are less than 40, insert the message on the cover image to make it equal to 40. To represent each group of two bits with an equivalent decimal number, convert the message to binary and create two-bit groups. Each pixel should be multiplied by the decimal equivalent of its R, G, and B values. A BIT WISE SHARING algorithm was used for visual cryptography. Shares of the image are divided into seven. Every pixel position in each share has some bit values that are missing. One share does not provide us with all the information we need in this case. The shares should be stacked correctly until four are stacked correctly. In order to reconstruct the image, a BITWISE OR operation must be performed. The secret message is retrieved from the cover image by searching for all pixels where two of the values of R, G, and B are equal to 40 and another value is equal to any of the set {40,41,42,43}. From these pixels, determine the comparable binary pattern and then express the additional value. The process should be repeated until all the binary patterns are obtained.

Furthermore, Islam et al. [31], developed a technique that uses text as well as an image as a secret message and cover object. In order to hide the secret text, first convert it into a QR code image. The cryptographic key in visual cryptography is generated using a random image called share1. 24-bit color images are used in visual cryptography. Red, green, and blue layers are created by dividing Share1 into a binary matrix and dividing the secret image into layers. A XOR operation is then performed on each of the corresponding layers between the secret image and the share1 image, creating a new image called share2 of the same size as the share1 image and the secret image. When share1 and share2 are combined, the secret image will be revealed. Share2 does not reveal any confidential information. The cover image and the share2 image are divided into green, red, and blue layers using the steganography technique. By replacing each LSB bit of a pixel of the cover image with each bit of the share2 image in sequence, each layer of the share2 image is concealed in the corresponding layer of the cover image. For each pixel in the share2 image that needs to be hidden, we need to subtract 8 pixels from the cover image. This method provided good security for the secret image.

Additionally, Hossain [32], developed an algorithm called the ElGamal ECC technique, which is used to implement encryption in the initial phase of the algorithm. Users receive their unique private keys in order to meet the requirement for secure cloud data sharing. The sender and the recipient are the initial stakeholders in the process, and the sender wishes to communicate files to the recipient in a secure manner. Using the curve method, a user (who may be the sender or the recipient) generates an ElGamal key pair consisting of a private and public key and then distributes these keys to one another. These keys are then used to encrypt the original message, which is later decrypted. Afterward, the ciphertext is encoded (encrypted) using the ElGamal public key. Using the Masking Filter steganography technique, the encrypted ciphertext is then concealed by an image. Steganographic images are the preferred technique for authentication. After receiving the stego cipher image, the receiver extracts the ciphertext from the stego cipher image. This model concludes with the recipient decrypting the ciphertext with the private key and receiving the original plaintext. The process should be repeated until all the binary patterns are obtained. Table 1 summarizes all previous literature reviews.

Table 1. Using Visual Cryptography and Steganography in Cloud

Refs.	Problem	Solution	Advantage	Disadvantage	Used Algorithms
[21]	Because its structure relies on mathematical computations, modern data security techniques could be breached.	The basic concept is to embed the sensitive object into the host medium without pre-encrypting the secret data.	Embedded objects can be any data.	Due to the algorithm's one-by-one processing, there is a very high level of temporal complexity.	Quantum walk (QW)
[22]	Increase the load on the processor to slow down the processor and this affects performance.	Employed the idea of a key to solve this issue. Now, the key is contained as an image together with the information or data itself.	Enhances the effectiveness of cloud computing and increases trust in mobile computing.	The system has no mechanism for recovering the key, hence in this scenario, a user might cause the data to be lost, limited data.	The least significant bit of technique
[23]	The problem of storing and most important and sensitive data on cloud storage.	Implement genetic algorithm and visual cryptography for storing such type of data on the cloud.	The security features of the genetic algorithm are highly enhanced with visual cryptography, which also gives overall minimum overhead.	Cannot access secret image information from parts less than k.	Genetic Algorithm Visual Cryptography

Refs.	Problem	Solution	Advantage	Disadvantage	Used Algorithms
[24]	Phishing attacks, Security breaches.	By using the extended (VC) for uploading and downloading secret information, the (UEVCESAPDFCS) technique can effectively replace the use of conventional encryption calculation.	Hide a bigger sum of data with minimal effort, space, and time complexity, and recover the entire set of data with information secrecy.	This method has a huge calculation.	UEVCESAPDFCS algorithm SPDFUEVC algorithm
[25]	Privacy problems during the transfer of confidential data, as well as the problem of data theft.	Hiding features of the secret image before splitting it into shares and hiding it in the second image.	Produce stego image with good quality.	Not suitable for all image formats, only BMP color format.	LSB Visual Cryptography
[26]	Image processing and confidentiality Issues, and image shares theft.	Using an image scrambling technique in which the location of the pixels is shuffled to provide additional protection for the Stego image.	It facilitates various experiments and also increases security by adding technology that has more randomness.	Distortion occurs in the Stego image that is produced.	XOR and One Time Pad (OTP) Algorithm LSB Visual cryptography
[27]	Privacy issues while transferring data or images.	The data is compressed using the LZW algorithm before being hidden in the image and encrypted.	This system secures data in the cloud environment and makes it more secure.	An increase in the amount of data size that can be hidden in the cover image.	AES256 RSA LSB
[28]	Facing the issue of data privacy and security for cloud customers.	Additional RGB shuffling using the least significant bit method contributes.	The resulting image is very close to the original quality.	The use of keys in this algorithm increases its size and execution time.	RGB shuffling Message Digest 5 (MD5) Least Significant Bit (LSB)
[29]	The breaches of security in the cloud service.	Implementation of a new steganography technique utilizing the International Data Encryption Standard Algorithm (IDEA) and the Least Significant Bit Grouping (LSBG) algorithm.	Offers enhanced embedding capacity, sufficient security, and minimal image distortion.	Privacy and confidentiality issues arise due to the use of simple data.	International Data Encryption Standard Algorithm (IDEA) Least Significant Bit Grouping (LSBG) algorithm

Refs.	Problem	Solution	Advantage	Disadvantage	Used Algorithms
[30]	Image privacy leakage and theft.	Steganography and visual cryptography were chosen for more secure data transmission with less computational risk over public media.	Compared with existing technologies, this technology generates shares with less space overhead and no increase in computational complexity and can provide better security.	The method cannot apply to colored shares just grey.	BITWISE SHARING BITWISE OR
[31]	When all the shares are piled up, the mystery of the image is revealed.	Ensures an extra layer of protection by using a pseudorandomly generated image as a visual encryption key.	The stego image that is produced is too clear to be undetectable by the human visual system.	It takes a long time to process.	XOR LSB
[32]	Privacy issues sometimes lead to data loss or modification by hackers and attackers.	Utilizes ElGamal Elliptic Curve Cryptography (ECC) for produces the tiny key by using the curve method.	Improvement in data privacy as well as reliability when sharing data on the cloud.	Storage and backup issues.	ElGamal Elliptic Curve Cryptography (ECC)

4. Conclusion

Researchers have proposed a variety of different techniques in the literature, which were reviewed in this paper. With clients frequently using the cloud to keep their information synchronized with the cloud, visual cryptography, and Steganography are among the latest technologies being used to cryptographically and hide data. In addition to providing customers and users with useful services, cloud computing has many benefits for the organization as well. When security problems are solved, cloud computing shows its glow in providing benefits to customers and users. However, cloud computing has faced security problems, most notably the lack of trust from users. Accordingly, from reviewing the different literature, we conclude that the techniques reviewed differ in implementation times as well as the complexity of calculations, and each technique has both strengths and weaknesses.

5. Acknowledgments

The authors are grateful to the reviewers and editors for their helpful feedback. The authors also extend their thanks to Altınbaş University and the supervisors of Dr. Oğuz Kara for providing the necessary support that led to the fruitful completion of this study. Thanks also to Dr. Yassen Hikmat for providing some valuable ideas.

6. References

[1] K. C. Nunna and R. Marapareddy, “Secure data transfer through internet using cryptography and image steganography,” *Conf. Proc. - IEEE SOUTHEASTCON*, vol. 2, 2020, doi: 10.1109/SoutheastCon44009.2020.9368301.

[2] A. A. Farsole, A. G. Kashikar, A. Zunzunwala, S. Nagar, and G. Chowk, “Ethical Hacking Ethical Hacking Procedure Certified Ethical Hacking Ethical Hacking : Future 15,” *Int. J. Comput. Appl.*, vol. 1, no. 10, pp. 14–20, 2010.

[3] L. Zhou, A. Fu, S. Yu, M. Su, and B. Kuang, “Data integrity verification of the outsourced big data in the cloud environment: A survey,” *J. Netw. Comput. Appl.*, vol. 122, no. July, pp. 1–15, 2018, doi: 10.1016/j.jnca.2018.08.003.

[4] P. Gadilkar, P. Gunjal, and N. Kamble, “Providing Data Security to File Backup System using Visual Cryptography in Cloud,” vol. 6, no. 7, pp. 113–115, 2019.

[5] T. Bolton, T. Dargahi, S. Belguith, M. S. Al-Rakhami, and A. H. Sodhro, “On the security and privacy challenges of virtual assistants,” *Sensors*, vol. 21, no. 7, pp. 1–19, 2021, doi: 10.3390/s21072312.

[6] R. Adee and H. Mouratidis, “A Dynamic Four-Step Data Security Model for Data in Cloud Computing Based on Cryptography and Steganography,” *Sensors*, vol. 22, no. 3, pp. 1–23, 2022, doi: 10.3390/s22031109.

[7] A. Fernández, D. Peralta, F. Herrera, and J. M. Benítez, “An overview of e-learning in cloud computing,” *Adv. Intell. Syst. Comput.*, vol. 173 AISC, pp. 35–46, 2012, doi: 10.1007/978-3-642-30859-8_4.

[8] A. S. Hashim, “A Review of Various Steganography Techniques in Cloud Computing,” *Univ. Thi-Qar J. Sci.*, vol. 7, no. 1, 2019, doi: 10.32792/utq/utjsci/vol7/1/19.

[9] M. K. Srinivasan, K. Sarukesi, P. Rodrigues, M. S. Manoj, and P. Revathy, “State-of-the-art cloud computing security taxonomies - A classification of security challenges in the present cloud computing environment,” *ACM Int. Conf. Proceeding Ser.*, pp. 470–476, 2012, doi: 10.1145/2345396.2345474.

[10] C. Stergiou, K. E. Psannis, B. G. Kim, and B. Gupta, “Secure integration of IoT and Cloud Computing,” *Futur. Gener. Comput. Syst.*, vol. 78, pp. 964–975, 2018, doi: 10.1016/j.future.2016.11.031.

[11] B. B. Gupta and O. P. Badve, “Taxonomy of DoS and DDoS attacks and desirable defense mechanism in a Cloud computing environment,” *Neural Comput. Appl.*, vol. 28, no. 12, pp. 3655–3682, 2017, doi: 10.1007/s00521-016-2317-5.

[12] J. Zhou *et al.*, “CloudThings: A common architecture for integrating the Internet of Things with Cloud Computing,” *Proc. 2013 IEEE 17th Int. Conf. Comput. Support. Coop. Work Des. CSCWD 2013*, pp. 651–657, 2013, doi: 10.1109/CSCWD.2013.6581037.

[13] F. Antonolpoulos, E. G. M. Petrakis, S. Sotiriadis, and N. Bessis, “A physical access control system on the cloud,” *Procedia Comput. Sci.*, vol. 130, pp. 318–325, 2018, doi: 10.1016/j.procs.2018.04.045.

[14] C. Modi, D. Patel, B. Borisaniya, A. Patel, and M. Rajarajan, “A survey on security issues and solutions at different layers of Cloud computing,” *J. Supercomput.*, vol. 63, no. 2, pp. 561–592, 2013, doi: 10.1007/s11227-012-0831-5.

[15] M. Ali, S. U. Khan, and A. V. Vasilakos, “Security in cloud computing: Opportunities and challenges,” *Inf. Sci. (Ny).*, vol. 305, pp. 357–383, 2015, doi: 10.1016/j.ins.2015.01.025.

[16] Y. Zhang, F. Patwa, R. Sandhu, and B. Tang, “Hierarchical Secure Information and Resource Sharing in OpenStack Community Cloud,” *Proc. - 2015 IEEE 16th Int. Conf. Inf. Reuse Integr. IRI 2015*, pp. 419–426, 2015, doi: 10.1109/IRI.2015.71.

[17] R. Itm, “A REVIEW ON TWO-LEVEL SECRET MESSAGE ENCLOSURE,” vol. 2, no. 8, pp. 1708–1711, 2015.

[18] Ashutosh and S. D. Sen, “Visual cryptography,” *Proc. - 2008 Int. Conf. Adv. Comput. Theory Eng. ICACTE 2008*, no. 1, pp. 805–807, 2008, doi: 10.1109/ICACTE.2008.184.

[19] K. Liu and L. J. Dong, “Research on cloud data storage technology and its architecture implementation,” *Procedia Eng.*, vol. 29, pp. 133–137, 2012, doi: 10.1016/j.proeng.2011.12.682.

[20] P. Kresimir and H. Zeljko, “Cloud computing security issues and challenges Tetracom View project BusinessLogicIntegrationPlatform View project Kresimir Popovic Siemens 4 PUBLICATIONS 143 CITATIONS Cloud computing security issues and challenges,” *Ieeexplore.Ieee.Org*, no. June, p. 7, 2010, [Online]. Available: https://www.researchgate.net/publication/224162841.

[21] J. Fausto, L. De Oliveira, L. Demetrio, and S. Pacífico, “Jo urn a,” *Appl. Soft Comput. J.*, p. 105970, 2019, [Online]. Available: https://doi.org/10.1016/j.asoc.2019.105970.

[22] S. K. Singh, P. K. Manjhi, and R. K. Tiwari, "Cloud Computing Security Using Blockchain Technology," no. July, pp. 19–30, 2021, doi: 10.1007/978-981-33-6858-3_2.

[23] Mamta, M. D. Khare, and C. S. Yadav, "Secure data transmission in cloud environment using visual cryptography and genetic algorithm: A review," *Int. Conf. Innov. Control. Commun. Inf. Syst. ICICCI 2017*, pp. 1–4, 2019, doi: 10.1109/ICICCIS.2017.8660941.

[24] S. Mandal and M. A. Mahmood, "Utilizing Extended Visual Cryptography for Ensuring Safety and Accuracy of PDF File in Cloud Storage," *ETCCE 2020 - Int. Conf. Emerg. Technol. Comput. Commun. Electron.*, no. December, 2020, doi: 10.1109/ETCCE51779.2020.9350873.

[25] S. A. Ali and Y. H. Ismaiel, "ENHANCED STEGANOGRAPHY USING VISUAL CRYPTOGRAPHY," no. October, 2019, doi: 10.4206/aus.2019.n26.2.40.

[26] C. Rangaswamaiah, Y. Bai, and Y. Choi, *Multilevel data concealing technique using steganography and visual cryptography*, vol. 70. Springer International Publishing, 2020, doi: 10.1007/978-3-030-12385-7_53

[27] M. S. Abbas, S. S. Mahdi, and S. A. Hussien, "Security Improvement of Cloud Data Using Hybrid Cryptography and Steganography," *Proc. 2020 Int. Conf. Comput. Sci. Softw. Eng. CSASE 2020*, pp. 123–127, 2020, doi: 10.1109/CSASE48920.2020.9142072.

[28] R. Nur Hadisukmana, "An Approach of Securing Data using Combined Cryptography and Steganography," *Int. J. Math. Sci. Comput.*, vol. 6, no. 1, pp. 1–9, 2020, doi: 10.5815/ijmsc.2020.01.01.

[29] R. Shanthakumari and S. Malliga, "Dual-layer security of image steganography based on IDEA and LSBG algorithm in the cloud environment," *Sadhana - Acad. Proc. Eng. Sci.*, vol. 44, no. 5, pp. 1–12, 2019, doi: 10.1007/s12046-019-1106-0.

[30] U. K. Mondal, S. Pal, A. R. Dutta, and J. K. Mandal, "A New Approach to Enhance Security of Visual Cryptography Using Steganography (VisUS)," *arXiv Prepr. arXiv2103.09477*, 2021, [Online]. Available: https://arxiv.org/abs/2103.09477%0Ahttps://arxiv.org/pdf/2103.09477.

[31] M. A. Islam, M. A. A. K. Riad, and T. S. Pias, "Enhancing Security of Image Steganography Using Visual Cryptography," *Int. Conf. Robot. Electr. Signal Process. Tech.*, no. January 2022, pp. 694–698, 2021, doi: 10.1109/ICREST51555.2021.9331225.

[32] S. E. E. Profile, "ENHANCING PERFORMANCE OF DATA PRIVACY ON THE CLOUD USING Enhancing Performance of Data Privacy on the Cloud Using Cryptography with Steganography in Python," no. December 2022, 2023.

سرية البيانات السحابية المخزونة في السحابة بإستخدام الإخفاء والتشفير المرئي: مراجعة

أسماء يعرب البكري [1، 2]*، أوكز كاران [1]

[1] هندسة حاسبات ، قسم تقنيات المعلومات ، جامعة ألتن باش، اسطنبول، تركيا
[2] قسم علوم الحاسوب، كلية علوم الحاسوب والرياضيات، جامعة الموصل، الموصل، العراق

الخلاصة

برز أمن الحوسبة السحابية كواحدة من أهم الإتجاهات في قطاع تكنولوجيا المعلومات، وهي تستخدم على نطاق واسع في هذا القطاع، ولاسيما مع نمو المعلومات في السحابة .يعد أمر البيانات المخزنة في السحابة، وكذلك عند نقلها بين المستخدمين والخوادم أمراً مهما للغاية. يمكن تحقيق نقل البيانات بشكل آمن من خلال إستخدام تشفير المعلومات وإخفائها، وهي من أهم التقنيات لتأمين البيانات والمصادقة عليها بحيث يكون المرسل والمتلقي فقط على علم بالمعلومات المخفية وكذلك نقلها. في المقابل، يعتبر التشفير المرئي هو تقنية تشفير تقوم بتشفير البيانات. من خلال وجود هذين الفرعين المختلفين، يكون من الصعب على المهاجم الكشف عن سرية البيانات. الغرض من هذا الإستعراض هو مراجعة بعض طرق إخفاء البيانات والتشفير المرئي التي تم إقتراحها لتحسين أمان السحابة وجعلها أكثر أماناً ضد الهجمات الألكترونية والتنصت. الهدف الاساسي من هذه الدراسة هو التحقيق في إمكانيات البيانات المؤمنة، والتي يستخدمها الباحثون بشكل متكرر . بالإضافة الى ذلك، يتم التحقيق في مزايا وعيوب كل مجال من مجالات البيانات المؤمنة . من أجل تعزيز آليات الأمان، خلص هذا البحث إلى أنه يمكن دمج مناهج التشفير المرئي مع إخفاء المعلومات والحوسبة السحابية في مجال البيانات المومنة.