JOURNAL LA MULTIAPP

VOL. 05, ISSUE 04 (336-345), 2024
DOI: 10.37899/journallamultiapp.v5i4.1337

Cloud Data Protection Based on Crypto-Steganography Approach

Ethar Abdul Wahhab Hachim[1]

[1]*Department of Computer Science, College of Science, Mustansiriyah University Baghdad, Iraq*

**Corresponding Author: Ethar Abdul Wahhab Hachim*
Email: ethar201124@uomustansiriyah.edu.iq

Article Info

Article history:
Received 6 June 2024
Received in revised form 20 June 2024
Accepted 24 July 2024

Keywords:
Cloud Computing
Steganography
Data Security
LSB Technique

Abstract

The benefits are numerous for organizations and people who work and learn using or through computers, some of these are scalability, affordability and availability of cloud computing services. However, one of the biggest issues still being faced in this area is that of security, especially concerning data privacy, thus limiting the use of such technologies. This paper seeks to address these concerns by developing a new approach to increasing protection of data in the cloud through development of Crypto-Steganography. The proposed method involves a two-tiered security mechanism: first, the presented data is protected with the use of advanced TWOFISH encipherment, which makes the data completely non-interpretated in case it gets to the hands of the unauthorized users. After that the encrypted data is then steganograghically inserted into a color image through least significant bit approach, where changes of the least significant bits of the image pixels will contain the encrypted data. Such double-layered approach does not only mask the presence of such sensitive information, but also ensures that even if there is an attempted invasion, such data can hardly be retrieved without the decryption passkey. The proposed approach of Crypto-Steganography is thoroughly tested through experiments and evaluation of distortion measures such as Weighted PSNR, UIQ; and C4 similarity measure. As seen in the results, the approach preserves low distortion and the wPSNR values are within the range of 45 – 50 dB, suggesting that the quality of the images is well preserved.

Introduction

There are several security challenges for adopting the cloud computing, and the security requirements diverge depending on the different cloud service categories and service deployment models. The multi tenant and distributed nature of cloud computing, the ability of remote access to the services and the number of entities that involved in the process make the cloud environment naturally more exposed to both external and internal security attacks (Hachim et al., 2022; Patel et al., 2020). Therefore, it has become necessary to develop an approach or models that enhance data protection in the cloud environment. Crypto-Steganography approach can provide an additional layer of protection and enhance the security to cloud data. Steganography allows for the embedding of sensitive data within non-sensitive cover data (Hachim, 2024). For example, you can embed confidential documents or encryption keys into images, audio files, or other seemingly innocuous files. This way, even if unauthorized users gain access to the cloud data, they might not detect the hidden information. Before embedding sensitive data in the cover files, it's essential to encrypt the data. This adds an extra layer of security, making the hidden information useless without the decryption key. It's important to note that steganography is different from cryptography

ISSN: 2716-3865 (Print), 2721-1290 (Online)

(Kannadhasan & Nagarajan, 2021). While both are used to protect data, cryptography focuses on making the data unintelligible to unauthorized users through encryption, whereas steganography focuses on hiding the existence of the data itself. The major goal for steganography is providing a covert communication channel, allowing secret information to be transmitted or stored without attracting attention. It is often used in conjunction with encryption for added security, creating a two-layered approach to protecting sensitive data (Hachim et al., 2023; Iftikhar et al., 2023).This paper has been prearranged as follows: A basic introduction to Cloud Data Protection Based on Crypto Steganography Approach has been provided in the first section. Section two reviews the previous related works. While the third section explain the most important steganography techniques in more details (Dhawan & Gupta, 2021; Rahman et al., 2023). Section four explains the steps of the proposed approach and the experimental results are presented and interpreted in section five. Finally, the last part shows a conclusion of this paper.

Related Works

1n 2020 Hassaballah et al. (2021) suggest an image steganography method for IOT and cloud applications. They divided the cover images to three by three matrices and extracted the centre pixel and performed XOR operation by the loaded image and then shuffled by the position of the bit, finally embedded it in the original cover image (Hassaballah et al., 2021). In 2020 Poduval et al. (2020) suggested a composite cryptography and steganography system using different cryptography algorithms to store the file in a secure manner on the cloud. They used 3DES and AES cryptography algorithms and then encrypt the key using RSA algorithm. To achieve high level of security in client side and embedded the data to the cover image before sending to the server side (Poduval et al., 2020; Sun et al., 2020).

In 2020 Ferdous et al. (2020) suggested a mixture model for data security in cloud by using Digital Signature Algorithm (DSA) to create digital signature. Also they used Advanced Encryption Standard (AES) for encrypt it and Steganography for hiding the data in an image or audio file. Their work enhanced data security from hackers or outsiders and verifies the data ownership (Ferdous et al., 2020). In 2022 Mawgoud et al. (2022) suggested a steganography framework depend on deep learning in a cloud environment. The implementation of suggested framework used ad-hoc cloud platform and employ open-source tools and deployment of relevant data in the images by using of the trainable deep learning that consist of three layers (Mawgoud et al., 2022).

In 2023 Nabil & Herráiz (2024) designed developed a secure model to improve data privacy and security on cloud environment. Their secure model used a combination of the steganography and the cryptography to support the security in cloud environment. Advanced Encryption Standard (AES) and Rivest Shamir Adleman (RSA) are shared with the Least Significant Bit (LSB) technique give a strong and flexible secure model for cloud computing environment (Nabil & Herráiz, 2024).

Methods

Steganography is the process of embedded or hiding a secret message within a cover message (object) to keep the communication safe and avoid the malicious threats. Cover object can be different in nature such as audio, video, text or image; therefore, steganography become a momentous practice for data protection in cloud environment (Awotunde et al., 2022). Steganography process categorized into different types depend on its cover object category, the nature of embedding domain, method of embedding and method of extraction ways.

Image steganography states the process of hiding the secret message within the image itself. The particular image that used for that purpose is named the cover image while the image that got after the steganography process called the Stego-image. Image steganography has now

ISSN: 2716-3865 (Print), 2721-1290 (Online)

become more popular for two reasons; easy transmission by the different low cost devices for the multimedia content such as smart mobile phone or digital camera, and use it in many social-media applications such as WhatsApp, Twitter, Facebook and LinkedIn (Hashim et al., 2021). Figure 1 explains steganography algorithm classification.

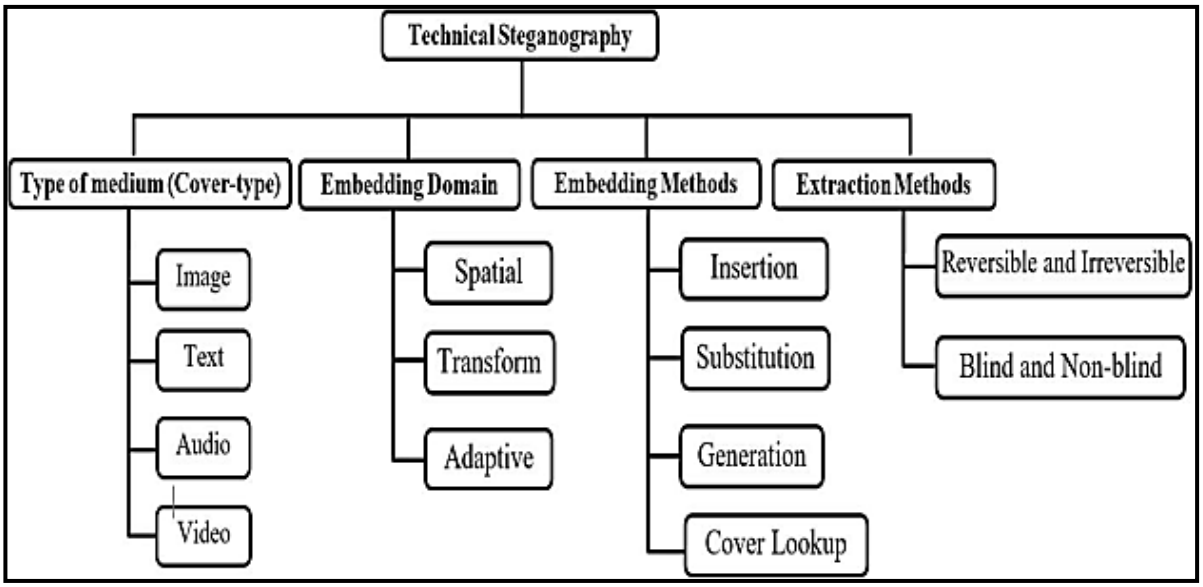


Figure 1. Classification of steganography algorithms [10]

Image steganography steps begin from embedded the secret message within the cover image by altering values of specific pixels depending on the used algorithm. Many techniques can be used for image steganography such as Masking and Filtering, Least Significant Bit, Coding and Cosine Transformation (Abikoye & Ogundokun, 2021).

Figure 2 explain the main steps for Image steganography process.

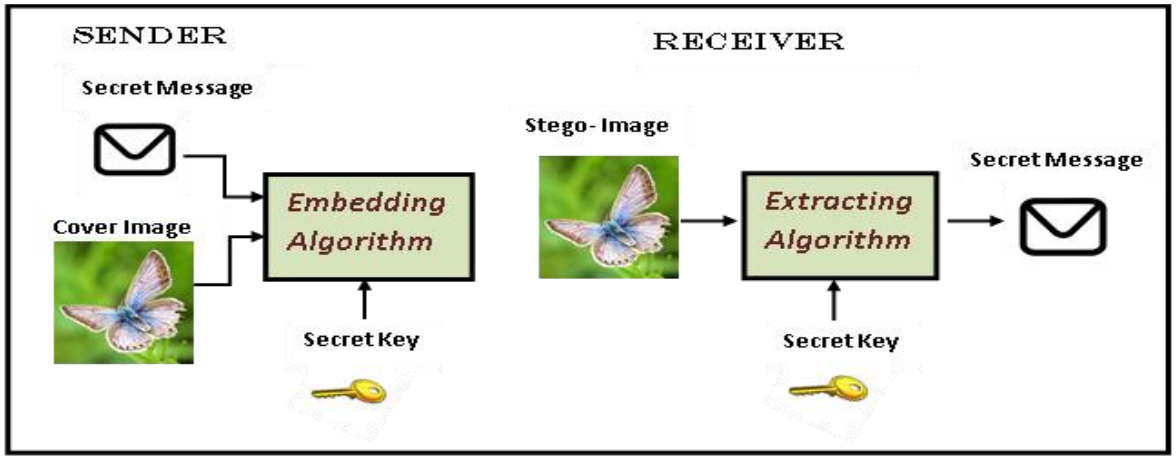


Figure 2. General steps of image steganography process

The Proposed Approach

In order to provide more protection and make the secret message unreadable before imbedded it to the cover image, it must be encrypted using TWOFISH block cipher technique which has many advantages as it provides a high level of security and efficiency. It is considered a fast encryption algorithm because it is a symmetric key block cipher, which makes it ideal for systems that deal with cloud environment that require rapid response and immediate interaction with client. The input secret message passes through sixteen round network that consist of many types of operation such as key scheduling, S-boxes, Pseudo-Hadamard Transform (PHT) and Maximum Distance Separable (MDS) matrices. Therefore, using of TWOFISH will ensure that the embedded message remains unreadable without the correct

ISSN: 2716-3865 (Print), 2721-1290 (Online)

decryption key even if it is discovered. Thus, using this encryption algorithm will provide additional layer of security to the proposed approach.

In this paper, RGB images used as a cover medium because its suitability for many applications and digital imaging devices, it is an ideal choice for steganography due to its ease of processing without causing noticeable distortions to the human eye. RGB image consist of three channels per pixels which help to offer multiple locations for imbedding the secret message by checking the pixel values in each channel. The pixel value in the red channel compared with its corresponding in the green and blue channels, and the smallest value among them will be selected to imbed the encrypted secret message bit using LSB technique then send it to the cloud. The original pixels values are indicated to use it later in the extracting phase by remove the additional values for the secret messages bits and restore original values. There are several steps can describe the whole approach: (1) First step: in this step the secret message (represent the sensitive data which is intended to de stored in the cloud) is encrypted by using TWOFISH encryption algorithm. That make this sensitive information unreadable even if it is discovered where it was embedded; (2) Second step: Preparing the embedding medium which is represented in this paper as a color image from Standard Image Dataset in RGB color model (If the image is in another color model such as YUV or HSV, the image can first be converted to RGB). Then separate the color image into three separate channels: blue (B), green (G), and red (R); (3) Third step: Use the Secret-key to generate the patterns that determine the hiding locations within the medium and assign the smallest value of the pixel in three channels in these locations by using the OpenCV libraries in Python to use it in embedding process; (4) Fourth step: In this step the encrypted secret message convert into a string of bits and embedded inside the cover image in the locations that were identified in the previous step. Least Significant Bit (LSB) technique used to modify the smallest bit in the selected pixel of the channel to make the changes more invisible and ensuring minimal distortion effects; (5) Finally, the Stego-image which containing hiding encrypted sensitive information is sent in secure way that ensures its safety in cloud environment.

Figure (3) shows in more details all the steps mentioned to implement this approach:

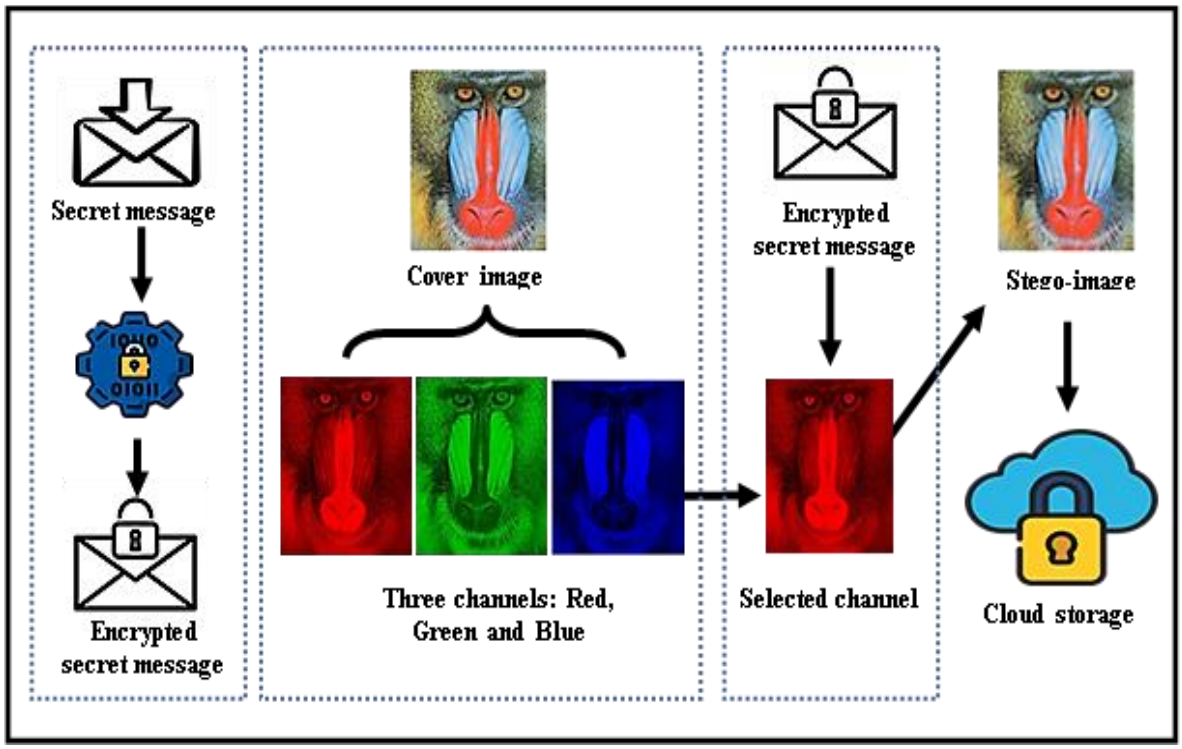


Figure 3. The proposed approach

ISSN: 2716-3865 (Print), 2721-1290 (Online)

The extraction process has been performing for retrieving the secret message exists in the Stego-image which obtained from the preceding phase. Actually, this phase consist of two steps, in the first step the encrypted secret massage take out from the Stego-image then, the decrypted process apply to it in order to find the original secret message.

As noted, the proposed approach consist of two basic phases (Embedding and Extracting), each one contains several steps that can be summarized in the two majors algorithms:

Embedding_Algorithm

Input: Original image (cover), Secret key, Secret message.

Output: the Stego-image

Begin

Step 1: Get secret massage and cover image in RGB form.

Step 2: Encrypted secret massage using TWOFISH encryption algorithm.

Step 3: Separate the original image in to three channels (blue_channel, green_channel, red_channel).

Step 3.1: For each channel, check the pixel value:

Step 3.1.1: Select the smallest value.

Step 3.1.2: Insert the encrypted secret message bits in the lower rightmost three bits for this pixel using LSB technique depending on secret key.

Step 3.2: Otherwise select Green channel and perform step 3.1.2

Step 4: Repeat the step 3 till all the characters of the secret message has been embedded.

Step 5: Merge all channels and obtain the Stego-image

End.

After the sensitive data reach the cloud, the receiver can retrieve it from the Stego-image by following steps mentioned in the following algorithm:

Extracting_Algorithm

Input: the Stego- image, Secret key.

Output: the Secret message.

Begin

Step 1: Get the Stego- image from receiver side.

Step 2: Separate the original image in to three channels (Red, Green and Blue).

Step 3: Depending on secret key, detect the pixel where the secret message was embedded in each channel.

Step 4: Extract the secret message bit.

Step 4: Repeat the step 3 until all the characters of the secret message has been extracted.

Step 5: Obtain the secret message

Step6: Decrypt the secret message using TWOFISH encryption algorithm.

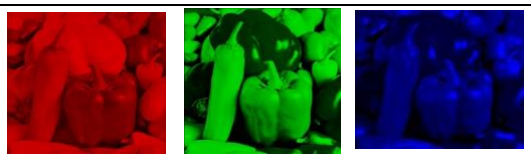
End

ISSN: 2716-3865 (Print), 2721-1290 (Online)

Results and Discussion

The implement of any steganography technique may cause distortion for the original image and this distortion must keep in the minimal. In order to prove the efficiency of this proposed approach, many different images were tested. Table 1 shows five of those images with their pre-processing operation and final results after embedding the sensitive data. The first column contains the cover images where the sensitive information to be hidden in them. The second column contains three channels for each image. While the third column contains the Stego-images that obtained after applying the embedding algorithm and contain the sensitive information before sending them to the cloud environment.

Table 1. Samples of images used in the proposed approach

NO.	Cover images	Processed images	Stego-images
1.1			
1.2			
1.3			
1.4			
1.5			

As noted in Table1, the resulting images (Stego-images) were not destroyed despite they inclusion of secret message within them and cannot be observed by the human eye. The distortion ratio is measured using different distortion metrics. Weighted Peak Signal-to-Noise Ratio (wPSNR) which consider enhancement of traditional PSNR used to improve the image quality measurement through giving the greater weight of the most visually important parts in the Stego-image. It is measured in decibels (dB) with a range from less than 20 dB (poor quality) to more than 50 dB (high quality) (Sahu & Sahu 2020). Universal Image Quality Index (UIQI) also used for measuring the similarity between the original (cover) image and the Stego-image to evaluate the effect of the noise and various distortions that may occur during steganography processing. UIQI values rang between (0) which indicates the presence of high distortion while (1) value indicates a perfect match between the two images (Jan et al., 2022). Another measure used to assess the similarity between two images is Mean Angle Similarity (C4) by analysing the angles between vectors representing pixel values. C4

ISSN: 2716-3865 (Print), 2721-1290 (Online)

provides greater independence from brightness and contrast differences because it depends on the angles between the vectors. It is also more sensitive to structural changes in the image. The (0) value indicate to complete matching between the two images, and the difference increases as the value of this measure increase (Mohamed et al., 2022). The proposed approach uses Standard Image Dataset in RGB color model size (512*512) from Kaggle dataset. The cover image preprocessing operations done using several OpenCV libraries in Python. Table 2 shows the wPSNR, UIQI and C4 values of the five different cover images and its corresponding Stego-images with the same secret message.

Table 2. wPSNR, UIQI and C4 values for the proposed approach

Image no.	wPSNR (dB)	UIQI	C4
1.1	48.786	0.995	0.98º
1.2	45.765	0.936	0.92º
1.3	46.786	0.952	0.93º
1.4	47.238	0.965	0.96º
1.5	47.659	0.973	0.97º

As can be noted from table (1) that the values wPSNR is near to (45-50) decibels (dB) is very acceptable and UIQI values and C4 values close to one for most images in the proposed approach. That mean it achieves hiding any secret message with a minimal distortion ratio of the original image and image resolution doesn't effected so much and is ignored when we embed any message inside the image.

The test results of this work confirm the efficiency of the developed Crypto Steganography in preserving the quality of an image and effectively placing information in an RGB image. The metrics adopted wPSNR, UIQI, and C4 suggest negligible loss in distortion, excellent image quality, and suitable hiding of the secret messages. These results are quite reasonable if to consider the main premises of steganography, in which one of the key points is the fact that the hidden data should be invisible, and the cover object's integrity should remain unaffected.

The proposed approach also shows competitive advantages compared to other recent methodologies as, for instance, those of Stević et al. (2020) and Poduval et al. (2020). The average wPSNR values found in this work are in the 45-50 dB range, hence the quality of the images is preserved better compared to the method developed by Stević et al. (2020) where XOR based embedding technique has slightly higher distortion. Also, integrating TWOFISH encryption with LSB embedding provides powerful security measures which is more secure than some of the hybrid cryptography steganography techniques that use simple AES encryption and LSB as explained by Poduval et al. (2020). Innovations in technology, including deep learning based steganography frameworks as put forward by Mawgoud et al. (2022) provide new areas of research to strengthen the data security in clouds. Nevertheless, these models tend to be more resource demanding in terms of computation and they may be difficult to run without prior professional experience. However, the proposed method offers a less complex yet efficient technique especially where computational time is of essence for instance in real time cloud services (Liu et al., 2022; Zhang et al., 2024).

The research findings of this study are therefore relevant to industries with cloud computing as their backbone in data management services. The Crypto Steganography approach makes it possible that any information subjected to the cloud will only be accessed be those with appropriate permissions regardless of anyone who may gain unauthorized access to the data. This two tier security measure encryption and then steganography offered a better safety way more so than encryption that has its open vulnerability to decryption in case the key gets in the wrong hands.

ISSN: 2716-3865 (Print), 2721-1290 (Online)

In addition, the approach can work with RGB imagery typical for digital media, which expands its usage to many cloud-based applications such as secure healthcare communication (Awotunde et al., 2022) and personal data protection in social media applications (Hashim et al., 2021). Since the inputs of standard image datasets and available libraries are easy to acquire, the proposed method can be easily implemented in existing cloud frameworks to be more scalable and efficient solution for data protection.

However, there are limitations in the findings of this study and they include the following. The current implementation is limited to RGB images, which most often might not be an appropriate choice depending on the type of data or industry (Fu et al., 2020). Further research should be carried out on its appropriateness to other media types including the audio or video files and its efficiency in such an environment. Furthermore, mainly caused by applying the LSB technique, described above, is that the approach is vulnerable to several steganalysis attacks focused on LSB-modified pixels. So, introducing new LSB or adding LSB with the new method might also improve the effectiveness of the proposed system, as Jan et al. (2022) proposed in 2022.

Conclusion

The main goal of storing data in the cloud is to achieve availability and access it at any time and from anywhere. The biggest challenge is how to keep the cloud data securely and protect it from cyber attacks. Therefore, maintaining the cloud data protection by using a Crypto-Steganography approach offers an effective solution for increasing data security and privacy in the cloud environment. The proposed approach aimed to build a robust crypto-steganography approach that relies on a secure hiding sensitive information in color images before sending them to the cloud with least distortions ratio as noted in the experimental result. Encrypting the secret message before imbedded it in the cover image had a significant impact for adding an extra level of security to protect it from any attempt to tamper these sensitive information.

Acknowledgment

The Author would like to thank Department of Computer Science, College of science, Mustansiriyah University, Baghdad –Iraq for its support to present this paper.

References

Abikoye, O. C., & Ogundokun, R. O. (2021). Efficiency of LSB steganography on medical information. *International Journal of Electrical and Computer Engineering (IJECE)*, *11*(5), 4157-4164. https://doi.org/10.11591/ijece.v11i5.pp4157-

Awotunde, J. B., Oladipo, I. D., AbdulRaheem, M., Balogun, G. B., & Tomori, A. R. (2022). An IoMT-based steganography model for securing medical information. *International Journal of Healthcare Technology and Management*, *19*(3-4), 218-236. https://doi.org/10.1504/IJHTM.2022.128195

Dhawan, S., & Gupta, R. (2021). Analysis of various data security techniques of steganography: A survey. *Information Security Journal: A Global Perspective*, *30*(2), 63-87. https://doi.org/10.1080/19393555.2020.1801911

Ferdous, J., Khan, M. F. N., Rezaul, K. M., Tamal, M. A., Aziz, M. A., & Miah, P. (2020). A Hybrid Framework for Security in Cloud Computing Based on Different Algorithms. *Int. J. Netw. Secur.*, *22*(4), 638-644. Https://doi.org/10.6633/IJNS.202007

Fu, L., Gao, F., Wu, J., Li, R., Karkee, M., & Zhang, Q. (2020). Application of consumer RGB-D cameras for fruit detection and localization in field: A critical review. *Computers and Electronics in Agriculture*, *177*, 105687. https://doi.org/10.1016/j.compag.2020.105687

ISSN: 2716-3865 (Print), 2721-1290 (Online)

Hachim E.A.W., Gaata, M.T. & Abbas, T. (2023). Voice-Authentication Model Based on Deep Learning for Cloud Environment. *International Journal on Informatics Visualization*, 7(3), pp. 864–870. http://dx.doi.org/10.30630/joiv.7.3.1303

Hachim, E. A. W. (2024). Cloud Data Protection Based On Crypto-Steganography Approach. *Journal La Multiapp*, *5*(4), 324-331. https://doi.org/10.37899/journallamultiapp.v5i4.1337

Hachim, E. A. W., Gaata, M. T., & Abbas, T. (2022, July). Iris-based authentication model in cloud environment (iamce). In *2022 International Conference on Electrical, Computer and Energy Technologies (ICECET)* (pp. 1-6). IEEE. https://doi.org/10.1109/ICECET55527.2022.9873499

Hashim, M. M., Mahmood, A. A., & Mohammed, M. Q. (2021). A pixel contrast based medical image steganography to ensure and secure patient data. *International Journal of Nonlinear Analysis and Applications*, *12*(Special Issue), 1885-1904. https://doi.org/10.22075/ijnaa.2021.5939

Hassaballah, M., Hameed, M. A., Awad, A. I., & Muhammad, K. (2021). A novel image steganography method for industrial internet of things security. *IEEE Transactions on Industrial Informatics*, *17*(11), 7743-7751. https://doi.org/10.1109/TII.2021.3053595

Iftikhar, A., Qureshi, K. N., Shiraz, M., & Albahli, S. (2023). Security, trust and privacy risks, responses, and solutions for high-speed smart cities networks: A systematic literature review. *Journal of King Saud University-Computer and Information Sciences*, 101788. https://doi.org/10.1016/j.jksuci.2023.101788

Jan, A., Parah, S. A., Hussan, M., & Malik, B. A. (2022). Double layer security using crypto-stego techniques: a comprehensive review. *Health and Technology*, *12*(1), 9-31. https://doi.org/10.1007/s12553-021-00602-1

Kannadhasan, S., & Nagarajan, R. (2021). Secure framework data security using cryptography and steganography in internet of things. In *Multidisciplinary approach to modern digital steganography* (pp. 258-278). IGI Global. https://doi.org/10.4018/978-1-7998-7160-6.ch012

Liu, Z., Xu, B., Cheng, B., Hu, X., & Darbandi, M. (2022). Intrusion detection systems in the cloud computing: A comprehensive and deep literature review. *Concurrency and Computation: Practice and Experience*, *34*(4), e6646. https://doi.org/10.1002/cpe.6646

Mawgoud, A. A., Taha, M. H. N., Abu-Talleb, A., & Kotb, A. (2022). A deep learning based steganography integration framework for ad-hoc cloud computing data security augmentation using the V-BOINC system. *Journal of Cloud Computing*, *11*(1), 97. https://doi.org/10.1186/s13677-022-00339-w

Mohamed, M. M., Ghoniemy, S., & Ghali, N. I. (2022). A Survey on Image Data Hiding Techniques. *International Journal of Intelligent Computing and Information Sciences*, *22*(3), 14-38. https://doi.org/10.21608/ijicis.2022.130393.1174

Nabil, B., & Herráiz, J. J. M. (2024). A Robust Cloud Security Model Leveraging a Hybrid of Cryptography and Steganography. *TechRxiv*. https://doi.org/10.22541/au.171221467.72775845/v1

Patel, A., Shah, N., Ramoliya, D., & Nayak, A. (2020, November). A detailed review of cloud security: issues, threats & attacks. In *2020 4th International conference on electronics, communication and aerospace technology (ICECA)* (pp. 758-764). IEEE. https://doi.org/10.1109/ICECA49313.2020.9297572

ISSN: 2716-3865 (Print), 2721-1290 (Online)

Poduval, V., Koul, A., Rebello, D., Bhat, K., & Wahul, R. M. (2020). Cloud based secure storage of files using hybrid cryptography and image steganography. *International Journal of Recent Technology and Engineering (IJRTE)*, *8*(6), 665-667. https://doi.org/10.35940/ijrte.F7227.038620

Rahman, S., Uddin, J., Zakarya, M., Hussain, H., Khan, A. A., Ahmed, A., & Haleem, M. (2023). A comprehensive study of digital image steganographic techniques. *IEEE Access*, *11*, 6770-6791. https://doi.org/10.1109/ACCESS.2023.3237393

Sahu, A. K., & Sahu, M. (2020). Digital image steganography and steganalysis: A journey of the past three decades. *Open Computer Science*, *10*(1), 296-342. https://doi.org/10.1515/comp-2020-0136

Shekhawat, V. S., Tiwari, M., & Patel, M. (2020). A secured steganography algorithm for hiding an image and data in an image using LSB technique. In *Computational Methods and Data Engineering: Proceedings of ICMDE 2020, Volume 2* (pp. 455-468). Singapore: Springer Singapore. https://doi.org/10.1007/978-981-15-7907-3_35

Stević, Ž., Pamučar, D., Puška, A., & Chatterjee, P. (2020). Sustainable supplier selection in healthcare industries using a new MCDM method: Measurement of alternatives and ranking according to COmpromise solution (MARCOS). *Computers & industrial engineering*, *140*, 106231. https://doi.org/10.1016/j.cie.2019.106231

Sun, S., Ma, H., Song, Z., & Zhang, R. (2020). WebCloud: Web-based cloud storage for secure data sharing across platforms. *IEEE Transactions on Dependable and Secure Computing*, *19*(3), 1871-1884. https://di.org/10.1109/TDSC.2020.3040784

Zhang, Y., Liu, B., Gong, Y., Huang, J., Xu, J., & Wan, W. (2024). Application of Machine Learning Optimization in Cloud Computing Resource Scheduling and Management. *arXiv preprint arXiv:2402.17216*. https://doi.org/10.48550/arXiv.2402.17216

ISSN: 2716-3865 (Print), 2721-1290 (Online)