ISSN 2047-3338

Triple Block Data Security Based on Distributed Crypto-Steganography in the Cloud Environment

[1]Derrick Méthode BAGAZA, [2]Blaise Omer YENKE, [3]Jean M'BOLIGUIPA
[1,3]Faculty of Science, University of Bangui, Central African Republic
[2]Department of Computer Science, University Institute of Technology, University of Ngaoundere, Cameroon

***Abstract*— Recent advances in cloud architecture led to the need to ensure more the privacy of data stored online. Data security is one of the most sensitive issues in Cloud environments. Indeed, users would like to have guarantees on the availability and integrity of their data. Multiple strategies have been deployed to achieve data security: making information completely unintelligible to unauthorised entities using cryptography, hiding the existence of information using steganography so that it cannot be detected, controlling access to information using blockchain technology and attribute-based encryption for secure interaction. Many authors have tried to reconcile steganography and cryptography by using ciphers or combinations of ciphers such as AES, RSA, Blowfish and the LSB technique. LSB has flaws due to the quality of additive noise which affects the statistical properties of the image. Furthermore, some authors have used the DCT technique, but DCT has limitations with respect to steganalysis when used alone. In this work, LSB and DCT techniques are combined for data integration and extraction to further enhance security. We call this combination LSB-DCT. Numerous experiments have been conducted to test the proposed approach and the results show a better data security performance index than the literature works.**

***Index Terms*— AES, Cloud Computing, Cryptography, LSB-DCT, RSA and Steganography**

I. INTRODUCTION

CLOUD computing is one of the most innovative IT models of recent years. It allows companies and organisations to use shared storage, computing resources, flexible, secure and cost-effective IT infrastructure [1]. This technology is bringing revolutionary changes and an ever-increasing amount of resources to IT sectors. Cloud has different types such as public cloud, private cloud, hybrid cloud, community cloud and different services including infrastructure as a service (IaaS), software as a service (SaaS) and platform as a service (PaaS) [2], [3]. One of the main advantages of this technology for firms is the reduction in the processing time of their submitted tasks and the reduction in investment costs.

Despite all the advantages of cloud computing, multiple security issues are nowadays drawing attention to data protection, network security, virtualization security, application integrity and identity management. Thus, researchers have found mechanisms such as cryptography, digital signature and steganography to solve these problems [4].

Cryptography and steganography are two techniques used to protect data from unauthorised intervention during transmission. Cryptography is a science that protects secret data by making the content unintelligible to unauthorised persons, while steganography is a process of hiding secret data in media that do not reveal its existence during data transfer. Common media used to carry the message or secret data are images, text or sound [4].

The authors of [4] presented an approach combining the MD5 cryptographic algorithm and RGB shuffling using the LSB technique. The latter guarantees security but has flaws with respect to steganalysis. According to [5], the authors proposed a system in which the Blowfish algorithm and the DCT steganographic method were employed to ensure data security. However, they noted limitations related to the use of a single key for encryption and decryption of data. The authors of [6] presented a security model where they used AES, RSA encryption and the LSB steganographic technique to protect data in the cloud. However, the latter has the shortcomings of the LSB technique as stated above. Since data security in the Cloud has already been the subject of much research, the question we try to answer in this modest work is whether designing a security model can improve security and ensure data privacy in Cloud environments. In this work, we propose an approach that combines cryptography and steganography

This work was supported by the LASE Laboratory of the University Institute of Technology, University of Ngaoundere, Cameroon and the Faculty of Science, University of Bangui, Central African Republic.

D. M. B. Author is with the Faculty of Science, University of Bangui, Central African Republic (Email: derrickmethodebagaza@gmail.com).

B. O. Y. Author is with the Department of Computer Science, University Institute of Technology, University of Ngaoundere, Cameroon (Email: boyenke@univ-ndere.cm).

J. M. Author is with the Faculty of Science, University of Bangui, Central African Republic (Email: jmboliguipa@yahoo.fr).

like the previous work but with a focus on steganography coupling two techniques LSB and DCT in order to solve the problems posed in [4], [5], [6] to improve data security in Cloud Computing environments. For the design of the said model, we used the research methodology of design science. In the proposed new approach, hybrid cryptography (AES-RSA) is reconciled with least significant bit techniques and discrete cosine transform (LSB-DCT). This combined approach guarantees confidentiality, integrity, capacity and robustness as the masking of the information is not visible, which also ensures the conformity of the stego image and the original image. Firstly, all users authenticate themselves using the SHA-2 algorithm, and secondly, AES-RSA cryptography and LSB-DCT techniques are used to encrypt the secret data and then merge it into the pixels of an image, thus forming a high level of security. The recovery of the secret data is done at the last block. Finally, the main objective of secret data protection is achieved by using conciliated approaches. This new approach provides data security in the cloud in three blocks namely authentication, encryption and recovery.

The rest of this paper is organized as follows: section II is dedicated to the literature review on data security in the cloud. Section III describes the proposed model and Section IV is dedicated to the analysis of the results. The conclusion and future work are presented in Section V.

II. REVIEW OF THE LITERATURE

Cryptography and steganography share the common goal of ensuring adequate data protection. These techniques have been the subject of several researches in the literature, where approaches to data security have been presented.

In [12], the authors proposed an approach that combines the snake cryptographic algorithm [21] and distributed steganography [12] to ensure the confidentiality and integrity of data in the cloud. The latter first encrypts the data using the snake algorithm and then the resulting ciphertext is subjected to distributed steganography using the least significant bit (LSB) technique to achieve a strong data security mechanism. In such a model, the LSB approach is declared vulnerable in the model proposed in [6].

The authors of [7] have developed a secure cryptographic system that uses a three-step user authentication process and automatic data encryption in the cloud. In fact, they use RSA or AES algorithms in their system.

In [8], [20], the authors implemented a security approach combining AES-256, RSA and LSB cryptographic algorithms for steganography to double the security of data in the cloud. They used a four-stage security model in conjunction with hybrid encryption, in which AES-256 and RSA algorithms were combined to ensure data security in the cloud.

In [10], the authors proposed a three-stage data security model in a cloud environment based on the RSA algorithm and LBS steganography. In this model, the data is encrypted first by the RSA algorithm, then the resulting cipher is subjected to steganography and then the stego image is sent to the receiver capable of retrieving the data from the symmetric key. However, there is a need to improve this combination to increase the security of the data.

According to [3], steganography is considered as a data security approach in cloud computing. However, they focus on the combination of LSB and DCT techniques to hide secret information in the pixels of the original image respecting a number of conditions in order to make the system effective.

The authors of [11] proposed an adaptive PVD (Pixel Value Differentiation) based approach for image steganography to embed the secret information in the cover image based on the difference between two neighbouring pixels.

The authors of [9] proposed a multi-layer security model to secure data transfer in the private cloud (SaaS). The first layer is responsible for intrusion detection and prevention, the second layer provides intrusion detection and prevention based on the Hidden Markov Model (HMM) [22], the third layer is responsible for data encryption using the AES algorithm and finally video steganography is performed at the last layer.

The authors of [13] proposed a new hybrid cryptography algorithm based on Blowfish, Rivest Shamir Adleman (RSA) and Secure Hash Algorithm-2 (SHA-2) algorithms for digital signature. The combination of these algorithms provides more data security but has vulnerabilities due to the LSB technique.

In [14], the authors implemented a new approach to steganography using the International Data Encryption Standard (IDEA) and the Least Significant Bit Grouping (LSBG) to embed and extract secret information. The combination of these two techniques with cryptography ensures the confidentiality and integrity of data in a system.

The authors of [15] showed that the main advantage of steganography over cryptography is that the secret message does not draw attention to itself because the message can be hidden under an image file, a video file, etc. They also showed that steganography can be used as an alternative to cryptography. They have also shown that steganography is an effective approach to hiding data when encryption is not allowed.

In [16], the authors proposed a method combining cryptography and image steganography. The secret message is encrypted by the Blowfish algorithm while the E-LSB technique of steganography is used to hide the data. Both methods provide better security of the data due to the PSNR values compared to other existing methods.

The authors of [17] presented a review on secure file storage in the cloud using hybrid cryptography. This system uses two different hybrid approaches for encryption and decryption, namely AES and RSA algorithms, and AES and Blowfish algorithms, and shows that both approaches provide high security, scalability, privacy in the Cloud.

Saleh et al [18] proposed a security model based on steganography and cryptography for the exchange of secret data in a cloud environment. This combined approach guarantees data security but has flaws related to the use of the unique key.

In [19], the authors used DCT, LSB and Blowfish steganographic techniques to provide high security. The Blowfish algorithm encrypts the secret data while the DCT technique hides the encrypted message in the cover image.

Algorithms presented in the literature have attempted to solve data security problems. However, they have flaws related to additive noise, steganalysis, and the use of single keys for encryption and decryption of data in the cloud. This paper highlights an approach to data security that combines hybrid cryptography and distributed steganographic techniques to address the security and privacy issues of cloud computing.

III. PROPOSED MODEL

In this section, we propose a new approach to data security combining hybrid cryptography and distributed steganographic techniques. The goal is to make secret data unintelligible and invisible in order to provide adequate security for sharing secret data online.

A. Overall architecture of the model

Hybrid cryptography is used to encrypt secret data using AES and RSA algorithms to achieve a higher level of security. In fact, it takes advantage of the interests of both symmetric and asymmetric encryption, such as the speed boost of symmetric encryption and the security of key sharing by asymmetric encryption.

Distributed steganography is therefore applied to encrypted data that is merged into the pixels of an image in order to protect it in a security-enhancing cover object using least significant bit (LSB) and discrete cosine transform (DCT) techniques. This combined approach of the two techniques aims to transmit data in such a way that no one can detect the existence of the data between a transmitter and a receiver.

We would like to remind you that at present, the cloud is attracting a lot of interest in data security, network security, virtualisation security, application integrity and identity management. As a result, several works have attempted to solve all these problems by using mechanisms such as cryptography, digital signature and steganography to solve these problems. However, the latter reveal some limitations presented above. To this end, the model proposed in this work will further enhance the security of data in the cloud. It is organized in three blocks, in which each of the blocks performs its function properly to ensure data security.

The first block is responsible for authenticating the user. The second block is responsible for the encryption and integration of the secret data into a cover object (media or image) for backup. The third block is responsible for the recovery and decryption of the secret data. With respect to this organisation, user authentication is used to verify that the data is not tampered with. Once the user authenticates, he or she can perform encryption and data integration operations. If a malicious entity gains access to the system using illegal means, encryption and data integration using cryptographic and steganographic algorithms can provide an additional layer of security. In this block, the data is encrypted by AES and RSA algorithms and then the resulting encryption is embedded in an image using the LSB-DCT technique, even if the user credentials have been used fraudulently, thanks to this block, the malicious entity will still not be able to access the secret data in the Cloud. Finally, data recovery, thanks to the LSB-DCT extraction algorithm, decryption by AES and RSA algorithms. This block allows the complete restoration of the data in case of damage. Fig. 1 shows the block diagram of the proposed model. It shows that the approach provides three-block security for data sharing and storage in the cloud.

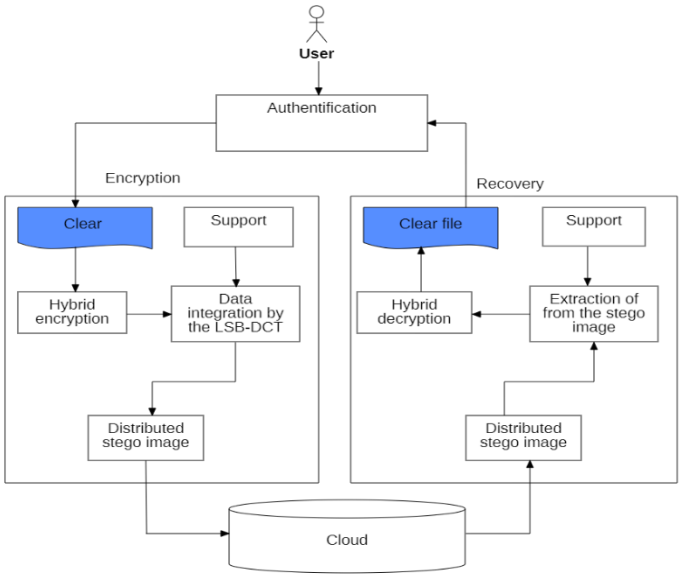

Fig. 1: Proposed architecture

B. Encryption and decryption process

This section presents in detail the encryption and decryption processes of the proposed model. First, we present the algorithms used in the different blocks of the model.

C. Phase 1: Authentication

Here, the authentication of the user is done in three steps. First, he provides his connection identifiers (login and password) then a key1 is generated using the identifiers provided previously thanks to the SHA-2 hash function. This key1 is sent by email to the user. Finally, the stored key1 is compared to the one sent to the user. In case of a match, a key2 is generated again using the anti-hash function of key1 followed by an update of key1 by key2. All these steps are described in Algorithm 1.

Algorithm 1 : Authentification

1. Provide login details
2. Generate a key1 using SHA-2 from the credentials and send it to the user
3. Compare the provided key1 to the stored one, if it matches, go to the next step, otherwise exit
4. Generate key2 using the anti-hash function of the user supplied key1, then update key1 with key2

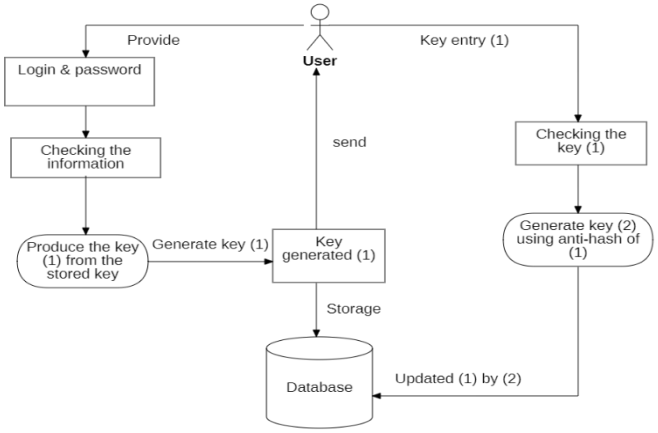

Fig. 2: Authentication process

D. Key generation algorithms

AES, also known as Rijndael, is a symmetric encryption algorithm that encrypts and decrypts data using the private or secret key. RSA is an asymmetric encryption algorithm that uses two keys, a public and a private key. The public key is known to everyone and is used to encrypt data while the private key is kept secret and is used to decrypt encrypted data. The key generation steps are shown in Algorithms 2 and 3.

Algorithm 2: AES key generation

1. Add an initial key
2. Perform a byte-by-byte substitution
3. Perform a row-by-row byte shift in the data block
4. Shuffle the bytes using the linear transformation
5. Combine the current round key with block values
6. Return the private key

Algorithm 3: RSA Key Generation

1. Choose two random primes p and q
2. Calculate the modulus of encryption n=p×q (by multiplying the primes p and q)
3. Compute φ(n)= (p-1) (q-1) (this is the value of the Euler indicator in n)
4. Choose a natural number e, such that e∈] 1, φ(n) [and gcd(e,φ(n))=1, called the encryption exponent
5. Compute the natural number d, such that e×d=1≡(modφ(n)), called thedecryption exponent
6. Return (n,e) and (d,n) as the public and private keys respectively.

E. Phase 2: Data encryption

In this phase, we use AES, RSA and LSB-DCT algorithms to encrypt and safeguard secret data to prevent exploitation by unauthorised persons in cloud environments. The process of encrypting secret data is presented by Algorithm 4. However, the algorithm uses data from Algorithms 2 and 3.

F. Data encryption algorithm AES-RSA and LSB-DCT

After generating the public and private keys, we will encrypt the data. Let's represent the encrypted file by F2 and the plaintext file (message) by F. The following figure illustrates the encryption process and the steps to be applied.

Algorithm 4: AES-RSA and LSB-DCT encryption

1. Generate an RSA master pair
2. Generate a random AES-256 key. It is a one-time use key
3. Select the text file F
4. Encrypt file F to F1 using the AES key
5. Encrypt the AES key using the RSA public key
6. Encrypt file F1 to F2 using the RSA public key
7. Save the encrypted AES key
8. Return file F2
9. Open the cover image and convert it to an RGB matrix (matrix that contains the colours of the image)
10. Read the F2 file and convert it to ASCII and then to binary
11. Apply DCT to the red matrix (extracted from RGB matrix)
12. Browse the original cover image pixel by pixel
13. Replace the least significant bit of the corresponding pixel in the original image with the corresponding message bit if the value of the coefficient corresponding to the scanned pixel is less than 0.
14. Write the distributed stego image
15. Save the distributed stego image in the Cloud.

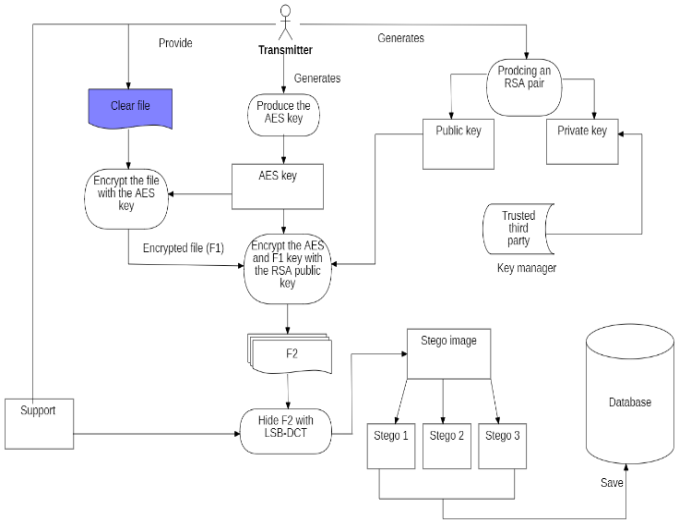

Fig. 3: Encryption process

G. *Phase 3: Data recovery*

To recover the secret data originally stored in the cloud, we will first reconstruct the stego image from the distributed stego images. The process of decrypting the secret data is summarised and illustrated by Algorithm 5 and Fig. 4.

Algorithm 5: AES-RSA and LSB-DCT decryption

1. Download the stego image distributed from the Cloud
2. Extract the F2 file from the stego image
3. Decrypt the AES key using the RSA private key
4. Decrypt file F2 into F1 using the RSA private key
5. Decrypt file F1 to F using the AES key
6. Return the file F

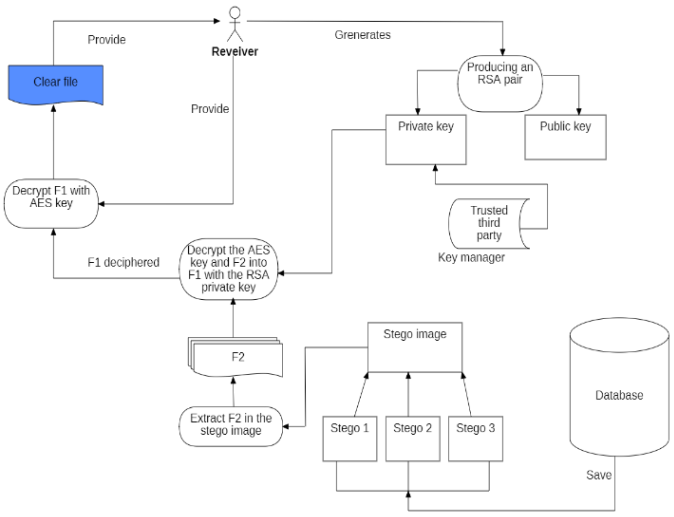

Fig. 4: Decryption process

IV. RESULTS AND ANALYSIS

The experiments were conducted on a 64 bit machine with 4 processors running at 2.40 Hz each. Python libraries were used to implement the proposed approach. This new approach ensures the protection of user data from unauthorised access. It increases the level of security in that it makes it difficult for unauthorised entities to decrypt the data in the cloud. Therefore, the reconciliation of AES-RSA and LSB-DCT encryption algorithms is considered an effective way to secure data.

A. *Evaluation of hybrid cryptography*

Cryptographic evaluations are made on the execution time in seconds by the size of the keys in number of bits when loading and downloading the data.

Table I: Execution time by key size in upload and download

Key size AES (in number of bits)	128	192	256	512	1024
Upload time (in seconds)	0.00042	0.00083	0.00155	0.003	0.006
Download time (in seconds)	0.00083	0.00164	0.0031	0.0065	0.013

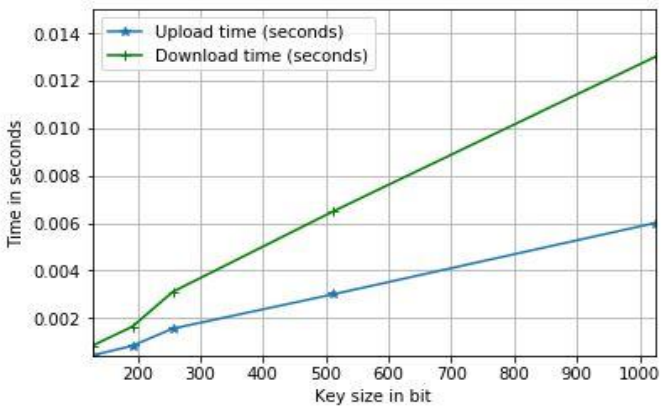

Fig. 5: Upload and download time by key size in bits

Fig. 5 shows the runtime required by a file with different AES key sizes for encryption. However, it shows that the data download time is greater than the upload time.

Hybrid cryptography actually has interests that symmetric and asymmetric encryption provide, such as the speed of symmetric encryption and the security of key sharing by asymmetric encryption. In addition, the data is encrypted from the sender to the receiver and the cloud is not aware of the decryption key.

The AES secret key used to encrypt the data is also encrypted with the robust RSA-4096 cipher and has never been broken before. The user must have access rights to the cloud. Fig. 6 shows the clear file and its encrypted file. These figures show the effectiveness of encryption in terms of data security.

Fig. 6: Secret data and encryption

B. *Evaluation of hybrid steganography*

Many parameters specify the quality of a steganographic system. In our work, the evaluation is done on a few. The results with each of the evaluated parameters are discussed in this section.

1) *Imperceptibility*

Imperceptibility is the quality of that which is imperceptible to our senses. This requirement is very important for a steganographic system. The proposed approach produces an imperceptible distributed stego image in which the hidden data cannot be observed by the human eye.

Fig. 7: Visual analysis

Fig. 7 clearly shows the results of the visual analysis of the proposed approach to the 'Lena' image. It shows no visual difference between the original image and the stego image. Thus, this approach holds up to sensitive attacks.

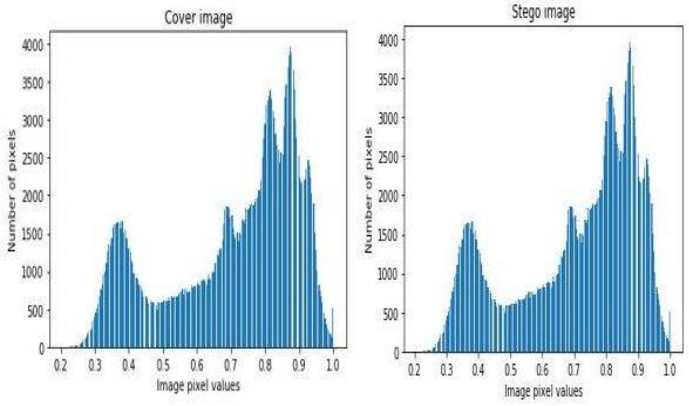

Fig. 8: Histogram analysis

Fig. 8 shows a graphical projection of the intensity values of the original image and the stego image. The x-axis represents the pixel values and the y-axis the number of pixels. The result of the histogram analysis clearly shows that the two images are identical and can in no way attract the attention of an attacker.

2) *Mean Square Error*

The mean square error (MSE) provides the average of the squared errors between the cover image and the stego image. It is calculated by equation (1).

$$MSE = \frac{1}{n*m}\sum_{i=1}^{n}\sum_{j=1}^{m}\left(V_{ij} - V'_{ij}\right)^2 \qquad (1)$$

where V_{ij} and V'_{ij} represent the pixel values of the cover image and the stego image. m and n represent the number of rows and columns respectively of the cover image.

3) *Maximum signal to noise ratio*

The maximum signal to noise ratio (PSNR) is a parameter that measures the quality between two images and is measured in decibels. It is calculated by equation (2).

$$PSNR = 10\log 10(255^2/MSE) \qquad (2)$$

More than ten simulations were performed on the image named "Lena", collected from the reference data sets (kaggle). The quality of the stego image is better due to the fact that the PSNR value is more or equal to 55.08 dB and a very low MSE value of 0.04.

Table II: Comparison of PSNR values of existing approaches

Authors	Techniques	Test images	PSNR (dB)
Mandal and *al*(2012)	Adaptive PVD	Lena	42,3
Saleh and *al* (2016)	Crypto_stegano	Lena	44,96
R Shanthakumari and *al* (2019)	IDEA-LSBG	Lena	54,85
Bagaza and *al*	LSB-DCT	Lena	55,11

Table II shows the PSNR values of different approaches in the literature. Our approach provides a very good PSNR value with an excellent image property. The PSNR obtained is 55.11dB, better than that of adaptive PVD, crypto-stego and IDEA LSBG which have PSNR values of 42.3, 44.96 and 54.85 respectively.

We can say that the proposed approach provides better results in terms of PSNR. On average, a PSNR of 55.09dB is obtained,

which implies a significant performance. With the combined approaches of cryptography and distributed steganography, data security is achieved in the cloud environment.

V. CONCLUSION

This paper proposes a new approach that includes distributed steganography and cryptography to secure data in cloud computing environments. For this purpose, we used RSA algorithm combined with AES algorithm and distributed steganography with LSB-DCT technique to hide the data so that unauthorised persons cannot access the original content. Considering the different approaches and methods used, the proposed model provides a very good PSNR value which guarantees the robustness of the proposed approach. Moreover, the PSNR obtained through the proposed model is superior to the one of works in the literature. Therefore, the model developed in this work can be used to further guarantee security in Cloud environments.

REFERENCES

[1]. Yagoub, M. A. (2019). *Une approche basée agent pour la sécurité dans le Cloud Computing* (Doctoral dissertation, Université Mohamed Khider de Biskra).

[2]. Kartit, Z., Azougaghe, A., Kamal Idriss, H., El Marraki, M., Hedabou, M., Belkasmi, M., & Kartit, A. (2016). Applying encryption algorithm for data security in cloud storage. In Advances in Ubiquitous Networking: Proceedings of the UNet'151(pp. 141-154). Springer Singapore.

[3]. SM Jahidul Islam, Zulfiker Haider Chaudhury, and Saiful Islam. (2019). A simple and secured cryptography system of cloud computing. In *2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE)*, pages 1–3. IEEE.

[4]. Rosalina, N. H. (2020). An approach of securing data using combined cryptography and steganography. International Journal of Mathematical Sciences and Computing (IJMSC), 6(1), 1-9.

[5]. Monika Gunjal and Jasmine Jha. (2014). Image steganography using discrete cosine transform (DCT) and blowfish algorithm. *International Journal of Computer Trends and Technology (IJCTT)*, 11(4):144–150.

[6]. Rose Adee and Haralambos Mouratidis. (2022). A dynamic four-step data security model for data in cloud computing based on cryptography and steganography. *Sensors*, 22(3):1109.

[7]. Aya Y AlKhamese, Wafaa R Shabana, and Ibrahim M Hanafy. (2019). Data security in cloud computing using steganography: a review. In *2019 International Conference on Innovative Trends in Computer Engineering (ITCE)*, pages 549–558. IEEE.

[8]. Shruti Kanatt, P Talwar, and A Jadhav. (2020). Review of secure file storage on cloud using hybrid cryptography. *Int. J. Eng. Res*, 9:16–20.

[9]. Suyash S Ghuge, Nishant Kumar, S Savitha, and V Suraj. Multilayer technique to secure data transfer in private cloud for saas applications. (2020). In *2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)*, pages 646–651. IEEE.

[10]. Vinay Kumar Pant, Jyoti Prakash, and Amit Asthana. Three step data security model for cloud computing based on RSA and steganography. In *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)*, pages 490–494. IEEE, 2015.

[11]. Mandal J K and Das D. (2012) Steganography using adaptive pixel value differencing (APVD) for gray images through exclusion of underflow/overflow. Computer Science & Information Technology, CSCP Series, pp. 93–102, ISBN: 978-1-921987-03-8

[12]. Peter Odion Izevbizua. (2015). Data security in the cloud using serpent encryption and distributed steganography. *European Scientific Journal*, 11(18):5845.

[13]. Nancy Garg and Kamalinder Kaur. (2016). Hybrid information security model for cloud storage systems using hybrid data security scheme. *International Research Journal of Engineering and Technology (IRJET)*, 3(4):2194–2196.

[14]. Shanthakumari, R., & Malliga, S. (2019). Dual-layer security of image steganography based on IDEA and LSBG algorithm in the cloud environment. *Sādhanā*, *44*(5), 1-12.

[15]. Aditya Poduval, Abhijeet Doke, Hitesh Nemade, and Rohan Nikam (2019). Secure file storage on cloud using hybrid cryptography. *International Journal of Computer Science and Engineering*, 7.

[16]. Kaur, M., & Kaur, A. (2014). Improved security mechanism of text in video using steganographic technique. *Int J Adv Res Comput Sci Softw Eng*, *2*(10).

[17]. Divya Prathana Timothy and Ajit Kumar Santra. (2017). A hybrid cryptography algorithm for cloud computing security. In *2017 International conference on microelectronic devices, circuits and systems (ICMDCS)*, pages 1–5. IEEE.

[18]. Saleh M E, Aly A A and Omara F A. (2016). Data security using cryptography and steganography techniques. International Journal of Advanced Computer Science and Applications 7(6): 390–397

[19]. Kaur, H., & Rani, J. (2016). A Survey on different techniques of steganography. In *MATEC Web of Conferences* (Vol. 57, p. 02003). EDP Sciences.

[20]. Mohammad Obaidur Rahman, Muhammad Kamal Hossen, Md Golam Morsad, and Animesh Chandra. (2018). An approach for enhancing security of cloud data using cryptography and steganography with e-lsb encoding. *IJCSNS*, 18(9):85.

[21]. Anderson, R., Biham, E., & Knudsen, L. (1998). Serpent: A proposal for the advanced encryption standard. *NIST AES Proposal*, 174, 1-23.

[22]. Eddy, S. R. (2004). What is a hidden Markov model? *Nature biotechnology*, 22(10), 1315-1316.