Cloud Data Security System Using Cryptography and Steganography: A Review

AKSA Anudini[1#], G. Gayamini [2], and Prof. Thushara Weerawardane [2]

[1]*Department of Computer Science, General Sir John Kotelawala Defence University, Sri Lanka*
[2]*Department of Computer Engineering, General Sir John Kotelawala Defence University, Sri Lanka[#]*
36-cs-0011@kdu.ac.lk

DOI: 10.29322/IJSRP.12.09.2022.p12936
http://dx.doi.org/10.29322/IJSRP.12.09.2022.p12936

Paper Received Date: 15th August 2022
Paper Acceptance Date: 15th September 2022
Paper Publication Date: 26th September 2022

***Abstract*— Data and information security can be considered one of the most important issues of the 21st century and it is essential to avoid data breaches, decrease the risk of data exposure, and ensure regulatory compliance. Cloud computing is a trending technology in this era. Cloud computing refers to the on-demand availability of digital resources, particularly data storage and computational power, without the user having to manage them directly. Cryptography and steganography can be defined as the most popular techniques that can be used to enhance data and information security inside the cloud. High-level security can be provided when cryptography and steganography are applied together to the cloud platform. Therefore, Hybrid cryptographic algorithms and multilayer steganographic techniques can be combined to develop a security system for efficient and secure data transmission in the cloud to provide availability, integrity, authenticity, confidentiality, and non-repudiation of the data and information. This paper analyzes the performance of cryptographic and steganographic techniques and suggests the best hybrid cryptographic algorithms and multilayer steganographic techniques that can be combined to efficient and secure data transmission in the cloud.**

Keywords— cryptography, steganography, Symmetric Key Cryptography, Asymmetric Key Cryptography, Image Steganography

I. Introduction

Cryptography is a technique of transforming secret information from readable to unreadable format and vice versa. Cryptography consists of terminologies namely plain text, ciphertext, encryption, and decryption. Converting a normal message (plaintext) into a meaningless message (ciphertext) is known as encryption and converting a meaningless message (ciphertext) into its original form (plaintext) is known as decryption.

Symmetric Key Cryptography (Private Key Cryptography) uses the same cryptographic key for both the encryption of plaintext and the decryption of ciphertext. Asymmetric Key Cryptography (Public Key Cryptography) has two keys namely private key and public key. The message will be encrypted by the sender using the public key of the receiver. Then the message will be decrypted by the receiver using his or her private key.

TABLE I. Comparison of Symmetric and Asymmetric Cryptography [1]

Symmetric Key Cryptography	Asymmetric Key Cryptography
Use the same key for both encryption and decryption	Use one key for encryption and another key for decryption
Fast encryption process	Slow encryption process
Provides confidentiality only	Provides confidentiality, non-repudiation, and authenticity
Used to transfer a large amount of data	Used to transfer a small amount of data
Low resource utilization	High resource utilization
Comparatively high security	Comparatively low security

Fig 1 shows the classification of cryptography based on the keys and encryption techniques used.

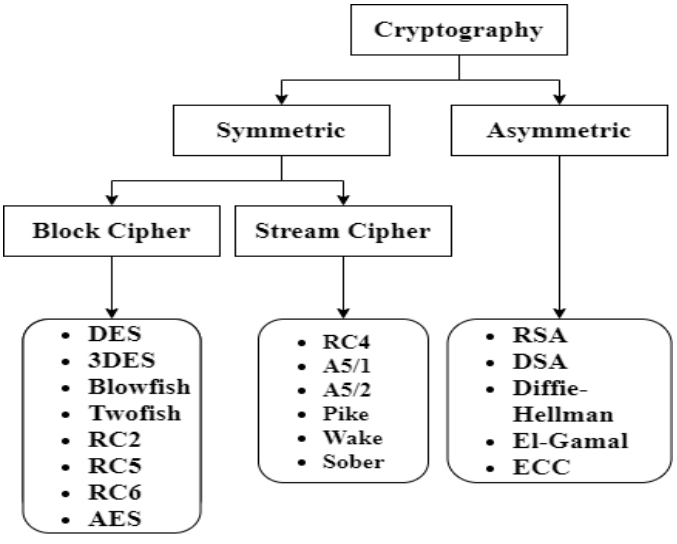

Fig. 1. Classification of Cryptography [2]

Steganography is an information hiding technique that uses cover objects to send messages between a sender and a receiver without making any suspicion and not allowing anyone else to know whether a communication is taking place. Steganography can be classified into five types depending on the nature of the cover object namely text, video, audio, image, and network steganography. Text steganography secures a message by hiding it in a specific letter of every word or by rearranging the text without changing its meaning. Audio Steganography makes use of the human ear to conceal information secretly. Video Steganography hides the secret message into a digital video. Network Steganography is the process of hiding information using a network protocol as a cover object, such as TCP, UDP, ICMP, IP, etc. Image Steganography hides the secret message in the cover object as an image.

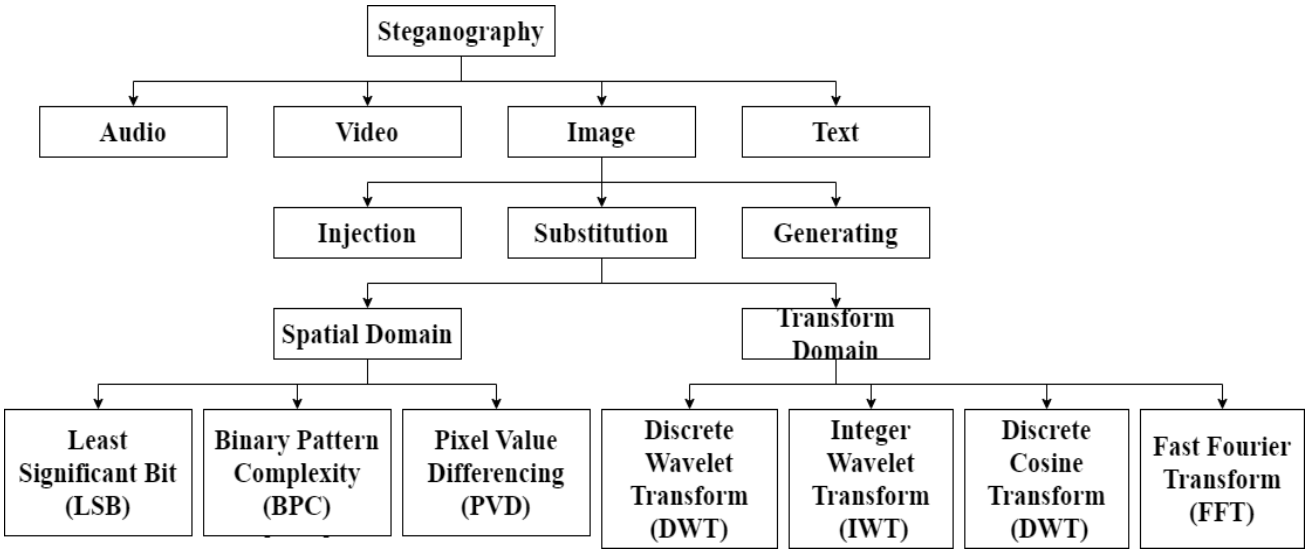

Fig. 2. Classification of Steganography [3]

Both steganographic and cryptographic approaches are used to secure data. Steganography differs from cryptography is where cryptography scrambles a message so that it cannot be understood by unauthorized users or third parties. Steganography camouflages to hide the existence of a message, then no one can know there is a secret message hidden in a cover object. Steganography provides confidentiality and authentication only while cryptography provides confidentiality authentication, data integrity, and non-repudiation.

Section II of this paper deals with the literature review on the researches related to data and information security using steganographic or cryptographic techniques. Section III provides the discussion and section IV presents the conclusion and further works.

II. Literature Review

This section deals with the vast number of researches that relate to secure and efficient data in the cloud using steganographic or cryptographic techniques.

Research on performance analysis of Symmetric Cryptographic Algorithms [4] has discussed different symmetric key cryptographic algorithms namely Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), Advanced Encryption Standard (AES), and Blowfish by analyzing encryption time, decryption time, avalanche effect, energy consumption, memory usage, and throughput by practical implementation using java. The results of the study reveal that the Blowfish algorithm requires less memory, high throughput, and it needs less time for the encryption and decryption of files when compared to other algorithms. Moreover, the study depicts that the blowfish algorithm is well suited for applications where memory and time usage play a significant role while the AES algorithm is ideal for applications where strength and the minimal energy consumption is crucial factor. In addition, DES is the best algorithm for applications that need security with minimal bandwidth consumption.

A study [5] was conducted to analyze the performance of asymmetric cryptographic algorithms namely Diffie-Hellman, RSA (Rivest, Shamir, Adleman), Elliptic-curve cryptography (ECC), El Gamal, and Digital Signature Algorithm (DSA) algorithms. The results of the study have concluded that each algorithm had its advantages and disadvantages. Furthermore, the experiments prove that the efficiency of RSA is lower than the ECC algorithm. In addition, El Gamal is slower in speed and DSA needs lots of time to authenticate and the verification process has complicated remainder operators. Moreover, the authentication procedure of the Diffie-Hellman algorithm is very low. Finally, the study concluded that the performance of all the algorithms varies upon the application they choose.

Research [6] proposed a method to provide high security to the cloud platform using double encryption techniques. The proposed system combined the AES symmetric cryptographic algorithm and RSA asymmetric cryptographic algorithm to increase the security and reduce the drawbacks of using those algorithms separately. The results of the study depict that the proposed methodology takes the least time for encryption runtime of the text file and decryption runtime of the text file.

In addition, the proposed system provides high security with resistance against propagation errors compared with DES, Blowfish, RC5, and 3-DES algorithms.

The study [7] aimed to create a new security solution to protect the data in the cloud with a hybrid cryptosystem. The proposed system combined the Blowfish symmetric cryptographic algorithm to ensure the confidentiality of data and the RSA asymmetric cryptographic algorithm to ensure the authenticity of data. In addition, this system consists of secure Hash Algorithm-2 (SHA-2) to ensure data integrity. Therefore, the study has revealed that this hybrid cryptosystem provides high security for data transmission over the cloud.

A review on data security in cloud computing using steganography [8] depicts the categories of steganography with a high focus on image steganography. The paper highlights the Discrete Cosine Transform (DCT) and Least Significant Bit (LSB) and the techniques. Performance evaluation of the spatial domain and transform domain techniques of image steganography exposed the fact that spatial domain, the LSB technique is mostly used to hide data that has a high payload capacity, but it's easily encoded and detected by attackers. In the transform domain, the DCT technique is very complicated and has a lower payload capacity compared to the LSB technique, but the DCT technique provides high security than the LSB technique. Furthermore, this research suggested that future work could combine LSB and DCT approaches to avoid the drawbacks that arise when applying these techniques individually and to provide more security to the secret message.

A study [9] analyzed the performance of Least Significant Bit (LSB), Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT) steganographic techniques. The performance analysis of the above-mentioned steganographic techniques was carried out by analyzing the parameters namely invisibility, robustness, Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE). Invisibility is the similarity of the stego image, and the original image. Robustness means the ability of the secret message to remain unchanged even if the stego image was subjected to changes. MSE is the square of the error between the cover image and stego image and PSNR can be defined as the ratio of the maximum signal to noise in the stego image. As a result of the experiments, it can be concluded that the DCT algorithm is the most suitable technique compared with the DWT and the LSB steganographic techniques.

Research [10] was conducted to analyze the performance of the LSB and modified DWT algorithm for image steganography. According to the results obtained by testing five RGB image sets, the researchers concluded that the modified DWT algorithm has a higher PSNR value, high security, invisibility, and robustness compared with the LSB algorithm. Furthermore, it was concluded that the overall performance of the modified DWT algorithm is better than the LSB algorithm.

Research [3] has exposed an efficient algorithm to provide the confidentiality, integrity, and authentication of data and information using hybrid cryptographic and steganographic algorithms. In this research, hybrid cryptography has been applied using AES symmetric cryptographic algorithm and RSA asymmetric algorithm. Then the secret message has been embedded using the LSB steganographic technique.

The study [11] focused on a cloud data security model using both cryptography and steganography. Through the proposed system data will be encrypted using the RSA asymmetric cryptographic algorithm. After that, the secret data will be embedded using Discrete Wavelet Transform (DWT) technique. Then the file will be uploaded to the cloud. The results of the proposed system will be provided with augmented security to the data and that can be used anywhere without qualms.

Another research [12] presented a multilayer security system to protect and hide multimedia data using cryptographic and steganographic techniques. Here, DES symmetric cryptographic algorithm is used as the symmetric cryptographic algorithm and the LSB technique is used to embed the secret message. Furthermore, the study has revealed that steganography is a highly effective technique used for confidential communications. In addition, the researchers concluded that the combination of cryptography and steganography can be used for many other applications apart from secret communications.

III. Discussion

Data security functions are used to avoid data breaches, decrease the risk of data exposure, and ensure regulatory compliance. The goal of data security in any organization is to assure the continuous safe and secure usage of private data while limiting the danger of exposure.

In recent years, people used symmetric or asymmetric cryptographic approaches to increase the efficiency and security of data transmission inside the cloud. But with the development of technology hackers easily broke the algorithms and decrypt the ciphertext. As a solution for using symmetric or asymmetric cryptographic algorithms individually, the researchers proposed systems to combine symmetric and asymmetric algorithms to enhance the security of the cloud. Therefore, the double encryption techniques using both symmetric-key algorithms and asymmetric key algorithms helps to reduce the drawbacks that arise when they are used separately. In the double encryption process, the two-time encryption and decryption process is performed using symmetric and asymmetric algorithms.

With technological advancement, cryptography was used along with steganography to give high security to the cloud. The fundamental drawback of cryptography is that anyone can understand there is a secret communication is taking place. As a result of that, hackers try to access the data by breaking the secret key. But when we use steganography, no one is aware of the ongoing secret communication. In this case, the secret message can be hidden inside audio, text, network, video, or image. The drawbacks that arise using only steganography to hide the secret message are steganography doesn't provide non-repudiation, and authenticity, it provides only confidentiality to the data. Therefore, to provide high security to data when saving, retrieving, and transmitting in the cloud, it is best to choose the best hybrid cryptographic algorithm and multilayer steganographic algorithm.

Table II shows the comparison of mainly using symmetric key cryptographic algorithms namely AES, Blowfish, DES, and 3-DES, and RC5.

TABLE II. COMPARISON OF SYMMETRIC CRYPTOGRAPHIC ALGORITHMS [4], [6]

Parameters	AES	DES	3-DES	RC5	BLOWFISH
Size of key and number of rounds	128,192 and 256 bits & 10,12 and 14 rounds respectively	64-bit key & 16 rounds	112 bits or 118 bits & 48 rounds	0 to 2040 bits & 12 rounds	32-448 bits, 16 rounds
Block size	128 bits	64 bits	64 bits	32, 64, or 128 bits	64 bits
Security	Secure	Not secure	Better than DES	Partially secure	Very Secure
Speed	Fast	Very slow	Slow	Slow	Fast
Data Confidentiality	Yes	No	No	No	Yes
Data Integrity	Yes	No	No	No	Yes
Cipher Text Size	Same as plain text	Larger than plain text	Larger than plain text	Larger than plain text	Same as plain text
Characteristics	Replacement for DES, Excellent security, flexible	Not much secure but flexible	Good security, Flexible	Not much secure, simple, consume less memory	Excellent security, Flexible

According to the previously discussed literature review and the comparison of the above-mentioned symmetric cryptographic algorithms, the best symmetric cryptographic algorithm that can be used is the Blowfish algorithm.

Table III shows the comparison of mainly using asymmetric key cryptographic algorithms namely Diffie-Hellman, RSA, ECC, EL Gamal, and DSA algorithms.

TABLE III. COMPARISON OF ASYMMETRIC CRYPTOGRAPHIC ALGORITHMS [5]

Parameters	RSA	DSA	ECC	Diffie-Hellman	El Gamal
Key size	>1024	1024	Calculates key from Elliptic curve equations	1024 to 4096	1024
Efficiency	Not very efficient	Very fast	Very fast and efficient	Not very efficient	Faster and efficient
Attacks	Brute force attack, a timing attack	The attacks may depend on the implementation	Doubling attack	Vulnerable to attack Man-in the-middle	Vulnerable to Meet-in-the-middle attack
Advantage	It is difficult to produce the private key from the public key and modulus. therefore, it provides high security.	Provide authentication and non-repudiation	Uses elliptic curve equations theory	The symmetric key is of very short length (256 bits); Therefore, the algorithm is quite fast	El Gamal encryption is different from El Gamal's signature. (Therefore, no confusion occurred)
Disadvantage	The complexity of generating keys is difficult	Needs lots of time to authenticate and the verification process has complicated remainder operators	It is complex, implementation is difficult	The authentication procedure is very low	Slower in speed, message expansion by a factor of two takes place in the encryption process

According to the previously discussed literature review and the comparison of the above-mentioned asymmetric cryptographic algorithms, the best asymmetric cryptographic algorithm that can be used is the ECC algorithm.

As discussed earlier, steganography can be classified as text, video, audio, network, and image steganography. Image steganography is the most popular steganographic technique because images are widely used, and they contain a large number of bits which used to hide a secret message. The image steganography techniques can be categorized as spatial domain and transform domain techniques.[8]

A. Spatial Domain Techniques

Secret messages are hidden directly in the intensity of pixels of the cover image in this method. Therefore,

embedding and extraction processes are very simple. These techniques are classified into several methods:

1) Least Significant Bit (LSB): In this approach, the secret message is embedded by replacing the least significant bits (bit number 8) of some or all of the bytes inside a cover picture. As a result, the LSB approach usually results in a large payload.

2) Binary Pattern complexity (BPC): The image complexity is used to determine the noisy blocks in the cover picture in this technique. The binary bits of the secret message is used to replace these blocks. This approach does not affect image quality degradation.

3) Pixel Value Differencing (PVD): The PVD separates the image into a series of non-overlapping two-pixel blocks and compares their differences. Although this method has a large capacity, it is not very secure.

B. Transform Domain Techniques

These methods give a high level of security. Rather than concealing the secret information directly in the pixels, the frequency coefficients of the picture are used in this method. It is complex to hide the secret message inside a cover image in transform domain techniques than spatial domain techniques.

1) Discrete Wavelet Transformation (DWT): DWT is frequently used for signal processing, watermarking, and image compression. The DWT mathematically decomposes an image into a series of functions known as wavelets.

2) Integer Wavelet Transformation (IWT): IWT technique will efficiently produce lossless compression. If the input consists of integers, the output will also consist of integers. As it translates integer to integer in the output, the IWT cannot lose data and it strengthens the security of the transformation.

3) Discrete Cosine Transformation (DCT): DCT technique can convert the image from the spatial domain to the frequency domain and split it into three frequency regions according to low frequency (FL), middle frequency (FM), and high frequency (HF).

To choose the best image steganographic technique it is necessary to consider the main steganographic characteristics. The main steganographic techniques are discussed here.

C. Invisibility

The similarity of the stego image and its related cover image is used to determine invisibility. As the similarity increases, the invisibility improves.

D. Payload

The number of secret bits that may be hidden in the cover image is referred to as the payload (capacity) and it is commonly measured in bits per pixel (bpp).

E. Robustness

The secret message can remain unchanged even if the stego image was subjected to changes such as linear and non-linear filtering, cropping, scaling and blurring, transformation, sharpening, etc.

F. Complexity

It measures the complexity of the steganographic algorithm.

G. Peak Signal to Noise Ratio (PSNR)

PSNR can be defined as the ratio of the maximum signal to noise in the stego image. It is one of the most well-known and widely used tools for evaluating the quality of stego images.

H. Mean Square Error (MSE)

MSE is the square of the error between the cover image and the stego image. If the MSE is smaller, then the image steganography technique is more efficient.

Table IV shows the comparison of main image steganographic techniques namely LSB, DCT, and DWT.

TABLE IV. COMPARISON OF IMAGE STEGANOGRAPHIC TECHNIQUES [9] [13]

Parameter	LSB	DCT	DWT
Invisibility	Low	High	High
Robustness	Low	Medium	High
Payload	High	Medium	Low
Complexity	Low	High	High
Peak Signal to Noise Ratio (PSNR)	Medium	High	Low
Mean Square Error (MSE)	Medium	Low	High

According to the previously discussed literature review and the comparison of the above-mentioned image steganographic techniques, the best hybrid steganographic technique that can be used is the combination of LSB and DCT algorithms. LSB technique has low invisibility and robustness while DCT has high invisibility and medium robustness. MSE value of DCT is low but LSB has a medium MSE value. Therefore, the combination of DCT and LSB techniques can reduce the drawbacks of using those algorithms separately.

IV. CONCLUSION AND FUTURE WORKS

Cloud security is a subset of cybersecurity that deals with policies, procedures, and technologies for safeguarding cloud computing systems. It protects data in the cloud and other digital assets from data breaches, distributed denial of service (DDoS), hacking, malware, and other cyber threats. This paper suggested using cryptography along with steganography to provide high-level security to the confidential data inside the cloud platform. Moreover, this review paper discussed the concept of cryptography, the performance of different symmetric and asymmetric key cryptographic algorithms, the concept of steganography, and the performance of different steganographic techniques. The facts discussed above proved that the blowfish algorithm has better performance when compared with other symmetric key cryptographic algorithms (AES, DES,3-DES, and RC5 algorithms). In addition, the ECC algorithm has better performance when compared with other asymmetric key cryptographic algorithms (Diffie-Hellman, RSA, ECC, EL Gamal, and DSA algorithms). Furthermore, it can be concluded that the combination of

LSB and DCT image steganographic techniques can provide extraordinary security when hiding the file inside a cover image. Future work can be done in a way of combining the blowfish symmetric key cryptographic algorithm and ECC asymmetric cryptographic algorithm as a hybrid cryptosystem to perform double encryption to secure the data. Then LSB and DCT image steganographic techniques can be combined to create a multilayer steganographic algorithm to hide the encrypted file to provide extra security. This proposed system will provide availability, integrity, authenticity, confidentiality, and non-repudiation to the data and information.

ACKNOWLEDGMENT

This research was supported by General Sir John Kotelawala Defence University, I would like to pay my gratitude to all the lecturers at the Faculty of Computing for the guidance provided throughout this research.

REFERENCES

[1] swetha vazhakkat, 'Difference between Steganography and Cryptography', Jun. 08, 2020. https://www.geeksforgeeks.org/difference-between-steganography-and-cryptography/

[2] E. Elgeldawi, M. Mahrous, and A. Sayed, 'A Comparative Analysisof Symmetric Algorithms in Cloud Computing: A Survey', *Int. J. Comput. Appl.*, vol. 182, no. 48, pp. 7–16, Apr. 2019, doi: 10.5120/ijca2019918726.

[3] C. Biswas, U. D. Gupta, and Md. M. Haque, 'An Efficient Algorithm for Confidentiality, Integrity and Authentication Using Hybrid Cryptography and Steganography', in *2019 International Conference on Electrical, Computer and Communication Engineering (ECCE)*, Cox'sBazar, Bangladesh, Feb. 2019, pp. 1–5. doi: 10.1109/ECACE.2019.8679136.

[4] S. Vyakaranal and S. Kengond, 'Performance Analysis of Symmetric Key Cryptographic Algorithms', in *2018 International Conference on Communication and Signal Processing (ICCSP)*, Chennai, Apr. 2018, pp. 0411–0415. doi: 10.1109/ICCSP.2018.8524373.

[5] S. Shakti, 'International Journal in Multidisciplinary and Academic Research (SSIJMAR) Vol. 4, No. 1, February 2015 (ISSN 2278 – 5973)', p. 6.

[6] K. Jaspin, S. Selvan, S. Sahana, and G. Thanmai, 'Efficient and Secure File Transfer in Cloud Through Double Encryption Using AES and RSA Algorithm', in *2021 International Conference on Emerging Smart Computing and Informatics (ESCI)*, Pune, India, Mar. 2021, pp. 791–796. doi: 10.1109/ESCI50559.2021.9397005.

[7] D. P. Timothy and A. K. Santra, 'A hybrid cryptography algorithmfor cloud computing security', in *2017 International conference on Microelectronic Devices, Circuits and Systems (ICMDCS)*, Vellore, Aug. 2017, pp. 1–5. doi: 10.1109/ICMDCS.2017.8211728.

[8] A. Y. AlKhamese, W. R. Shabana, and I. M. Hanafy, 'Data Securityin Cloud Computing Using Steganography: A Review', in *2019 International Conference on Innovative Trends in Computer Engineering (ITCE)*, Aswan, Egypt, Feb. 2019, pp. 549–558. doi: 10.1109/ITCE.2019.8646434.

[9] S. Chandran and K. Bhattacharyya, 'Performance analysis of LSB, DCT, and DWT for digital watermarking application using steganography', in *2015 International Conference on Electrical, Electronics, Signals, Communication and Optimization (EESCO)*, Visakhapatnam, Jan. 2015, pp. 1–5. doi: 10.1109/EESCO.2015.7253657.

[10] A. Singh, M. Chauhan, and S. Shukla, 'Comparison of LSB and Proposed ModifiedDWT Algorithm for Image Steganography', in *2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)*, Greater Noida (UP), India, Oct. 2018, pp. 889–893. doi: 10.1109/ICACCCN.2018.8748546.

[11] A. G. Palathingal, A. George, B. A. Thomas, and A. R. Paul, 'Enhanced Cloud Data Security using Combined Encryption and Steganography', vol. 05, no. 03, p. 4.

[12] D. Naidu, A. K. K S, S. L. Jadav, and M. N. Sinchana, 'Multilayer Security in Protecting and Hiding Multimedia Data using Cryptography and Steganography Techniques', in *2019 4th International Conference on Recent Trends on Electronics, Information, Communication & Technology (RTEICT)*, Bangalore, India, May 2019, pp. 1360–1364. doi: 10.1109/RTEICT46194.2019.9016974.

[13] H. B. MaciT, A. Koyun, and O. Güngör, 'A REVIEW AND COMPARISON OF STEGANOGRAPHY TECHNIQUES', p. 9.

http://dx.doi.org/10.29322/IJSRP.12.09.2022.p12936 www.ijsrp.org