iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** IX **Month of publication:** September 2023

DOI: https://doi.org/10.22214/ijraset.2023.55617

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue IX Sep 2023- Available at www.ijraset.com

Hybrid Encryption using LSB steganography and RSA

Vineela Reddy M [1], Anudeep Reddy G [2]
[1,2]*School of Computer Science and Engineering, VIT, Vellore*

Abstract: ***In the present world of communication, computers and the internet are the major media that connects different parts of the world as one global virtual world. So we can easily exchange lots of information within seconds of time, but the confidential data that needs to be transferred should be kept confidential. Thus, in order to aid this, we have proposed a new encryption technique by combining Image steganography (LSB) with the cryptographic RSA algorithm for providing more security to our data as well as imperceptibility. The expected outcome would be a properly secure combination of encryption models that uses steganography to hide the message content in a cover image, and also encrypts the message using the cryptographic algorithm, as an additional security layer, in case the content was retrieved from the cover image.***
Keywords: Cryptography, LSB, RSA, Steganography, PSNR, MSE.

I. INTRODUCTION

The basic need of every growing area in today's world is communication. This exchange of information must be secure and safe. In order to transport and share information in our daily lives, we use a variety of unsafe channels, including the telephone and the internet. Two techniques that are used to share information covertly are steganography and cryptography. A communication can be modified using cryptography such that it is protected by an encryption key that is only known to the sender and recipient. In contrast, steganography conceals the secret message in a cover image so that no intermediary can tell whether a message is hidden in the information being transferred. In cryptography, it is always obvious to an intermediary that the communication is in an encrypted form. The recipient is then given the cover image with the hidden message. The recipient uses the steganography algorithm to decode the message. It is a difficult technique that will require us to integrate two technologies: the RSA cryptographic method on the one hand, and the LSB steganography algorithm on the other. Our research has been concentrated on developing a method for securely transferring and sharing critical data. To prevent competitors or bogus parties from learning information about their company, all reputable businesses always encrypt data before transferring it over the internet. We have developed a secure steganography technique using LSB and RSA that is much more secure than many other systems used to covertly convey data.

II. LITERATURE REVIEW

Applications requiring high-volume embedding with robustness against certain statistical attacks have used the proposed approach. The current approach makes an effort to pinpoint what makes an effective data hiding algorithm. Additionally, it is meant to support cryptography and steganography rather than to replace them [1]. The embedding capacity grows when a message is encrypted and concealed using an LSB steganographic approach, allowing us to conceal vast amounts of data. Additionally, the technique fits the criteria for data concealment, including those for capacity, security, and robustness. The generated stego-image can be transferred covertly while yet maintaining confidentiality. Furthermore, even if an attacker were to defeat the steganographic technique to detect the message from the stego- object, Applications requiring high-volume embedding with robustness against certain statistical attacks have used the proposed approach. The current approach makes an effort to pinpoint what makes an effective data hiding algorithm. Additionally, it is meant to support cryptography and steganography rather than to replace them [1]. The embedding capacity grows when a message is encrypted and concealed using an LSB steganographic approach, allowing us to conceal vast amounts of data. Additionally, the technique fits the criteria for data concealment, including those for capacity, security, and robustness. The generated stego-image can be transferred covertly while yet maintaining confidentiality.

LSB based steganography embed the text message in LSB of cover image. The text message is hidden via DCT- based steganography in the LSB of the DC coefficients. This study applies LSB- and DCT-based steganography and computes the PSNR ratio. The peak signal to noise ratio (PSNR), expressed in decibels, compares two pictures. This ratio is used to compare the two photos' quality. Images are of higher quality if the PSNR ratio is high.

The PSNR ratio used to compare LSB-based and DCT-based stego photos reveals that the DCT-based steganography scheme has a higher PSNR ratio than the LSB-based steganography scheme for all types of images (Grayscale as well as Colour). DCT based steganography scheme works perfectly with minimal distortion of the image quality as compared to LSB based steganography scheme.[2] Despite the fact that less secret data may be concealed with this method than with an LSB-based steganography scheme, DCT-based steganography is still advised since it causes the least amount of image quality distortion.

The purpose of this work is to evaluate RSA, analyse its advantages and disadvantages, and suggest fresh remedies to address the disadvantage [3]. One of the most effective cryptographic methods now in use for ensuring secure network communication is RSA (Rivest, Shamir, and Adleman). Even though RSA is now the most popular cryptographic method, it has some drawbacks that must be taken into account if RSA is to remain the best, and work must be done to make RSA quantum resistant. Studies on quantum encryption techniques that are resistant to quantum computers are more important than ever because they will soon replace the existing encryption systems. Comparisons between the RSA and ECC ciphers show that the ECC has significantly lower overheads than RSA [4]. Due to its capacity to offer the same level of security as RSA while utilizing smaller keys, the ECC has been demonstrated to have numerous advantages. Its lack of maturity, however, may even mask its beauty because mathematicians felt that not enough research had been done on ECDLP. Additionally, we thought that even if both systems are legitimate, RSA is now superior to ECC because it is more dependable and its security can be trusted more. However, ECC's future appears more promising than RSA's because modern applications (such as smart cards, pagers, and mobile phones) cannot support the overheads that RSA introduces.

III. METHODOLOGY

A. Overall Architecture

The algorithm's fundamental structure is relatively straightforward. A text is entered by the user and transmitted to the recipient. The text is then encrypted and embedded in an image using LSB steganography. The image is transferred to the recipient, who decrypts the embedded bits to read the original message.

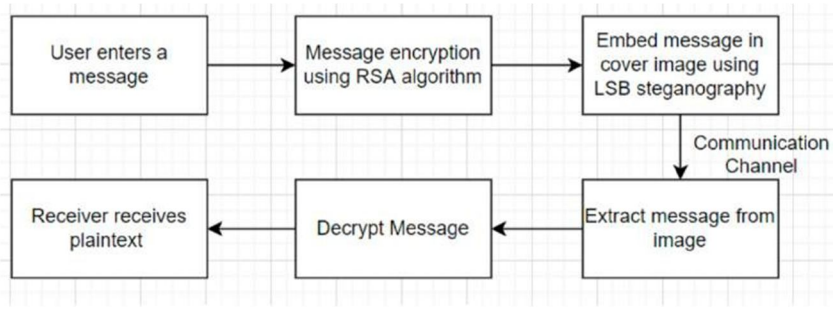


Fig 3.1.1 – Flow Diagram of data transfer process

B. RSA Algorithm

A public key and a private key are necessary for the asymmetric encryption method known as the RSA algorithm. The concept of RSA is based on the fact that big integers are challenging to factor. The public key is made up of two numbers, one of which is the product of two enormous prime numbers. The same two prime numbers are also used to create the private key. Therefore, the private key is compromised if someone is able to factorize the huge integer.

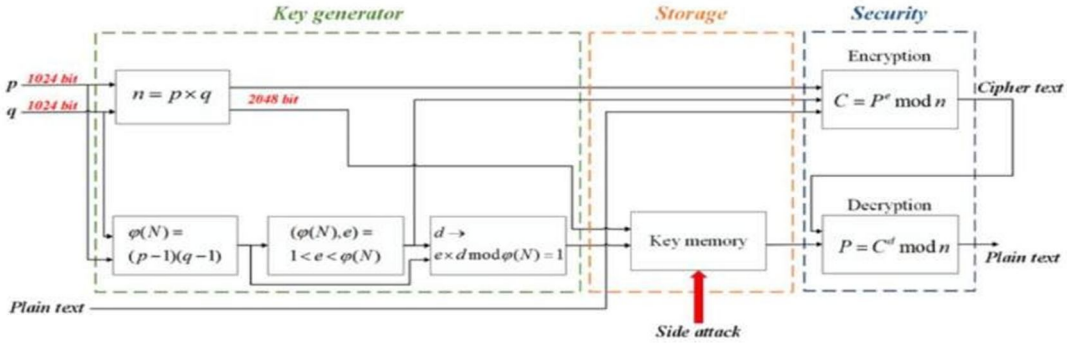


Fig 3.2.1 – RSA Algorithm

1) Select two large prime numbers, p and q.
2) Multiply these numbers to find n = p x q, where n is called the modulus for encryption and decryption.
3) Choose a number e less than n, such that n is relatively prime to (p - 1) x (q -1). It means that e and (p -1) x (q - 1) have no common factor except 1. Choose "e" such that 1<e < φ (n), e is prime to φ (n), gcd(e,d(n)) =1
4) If n = p x q, then the public key is <e, n>. A plaintext message m is encrypted using public key <e, n>. To find ciphertext from the plain text following formula is used to get ciphertext C. $C = m^e \bmod n$, Here, m must be less than n. A larger message (>n) is treated as a concatenation of messages, each of which is encrypted separately.
5) To determine the private key, we use the following formula to calculate the d such that: $D_e \bmod \{(p - 1) \times (q - 1)\} = 1$ or $D_e \bmod \varphi(n) = 1$
6) The private key is <d, n>. A ciphertext message c is decrypted using private key <d, n>. To calculate plain text m from the ciphertext c following formula is used to get plain text m. $m = c^d \bmod n$.

C. LSB Steganography

At its foundation, the idea that underlies image-based steganography is extremely straightforward yet incredibly adaptable. The discovery that an image's content, primarily the colours and visual features that humans see, is fundamentally defined by the digital data that makes up the image is at the core of this technique. In its purest form, an image is a mosaic of pixels, each of which contributes significantly to the final image. These pixels typically have three different values, which correspond to the red, green, and blue colours. The numerous hues and tints that give an image life are created when these RGB values are mixed in different ratios. The essence of image-based steganography lies in the recognition of this fundamental truth: that images are, at their core, composed of pixels. This realization opens up a world of possibilities for concealing and retrieving information within images. By subtly manipulating the RGB values of individual pixels, one can embed hidden messages, data, or even entire files within the seemingly innocuous facade of an image.

1) Encode the Data: Through the use of ASCII values, every byte of data is transformed into its 8-bit binary equivalent. Now a set of three pixels with a total of 9 values are read from left to right. Binary data is stored in the first 8 values. If 1 happens, the value becomes odd; if 0 occurs, it becomes even.
2) Decode the Data: Three pixels are read at a time during decoding, and when the last value is odd, the message is finished. The same encoding technique can be used to retrieve the binary data that each set of three pixels contains. The binary bit is 1 if the value is odd and 0 otherwise

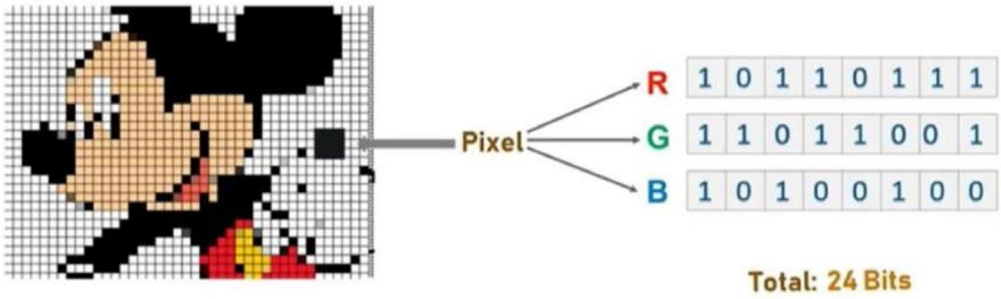


Fig.3.3.1 – 24-bit pixel representation

IV. RESULTS

1) *Sender Side*

```
Do you want to generate a new public and private key? (y or n) n
Would you like to encrypt or decrypt (e or d) e
What would you like to encrypt?
Hey
Enter the file name that stores the public key: public_keys.txt
Enter image name (with extension): mainimg.png
Enter the name of new image (with extension): stegimg.png
Max data encoded: 97864.66666666667
Encrypting...
Encrypted message is:  1550685 1224174
```

Fig 4.1 – Sender Side


Fig 4.2 – Cover Image 1


Fig 4.3 – Stego Image 1


Fig 4.4 – Cover Image.2


Fig 4.5 – Stego Image 2


Fig 4.6 – Cover Image 3


Fig 4.7 – Stego Image 3

2) Receiver's Side

```
Do you want to generate a new public and private key? (y or n) n
Would you like to encrypt or decrypt (e or d) d
What would you like to decrypt?

Enter image name (with extension): stegimg.png
Decrypting...
1550685 1224174
72101
121
Hey
```

Fig 4.4 – Receiver's side

A. Analysis

Peak signal-to-noise ratio (PSNR) is an engineering term describing the ratio of a signal's greatest power to the power of corrupting noise that degrades the representational accuracy of the signal. Due to the high dynamic range of many signals, PSNR is typically stated as a logarithmic number using the decibel scale. The reconstruction quality of pictures and videos that have undergone lossy compression is typically measured using PSNR. For a 24-bit image, a PSNR value between 70 and 90 is considered appropriate.

Image	PSNR	MSE
Purple Ring (Image 1)	72.4969	0.0037
Watercolour (Image 2)	77.0788	0.0013
Wings (Image 3)	75.1364	0.0019

Table 4.1.1 – PSNR and MSE Values of the three different images above

Length of Data (Characters)	PSNR	MSE
200	72.4969	0.0037
500	68.3861	0.0094
2000	62.3861	0.0374
5000	58.4552	0.0928
10000	55.4405	0.1858

Table 4.1.2 – PSNR and MSE w.r.t length of data embedded

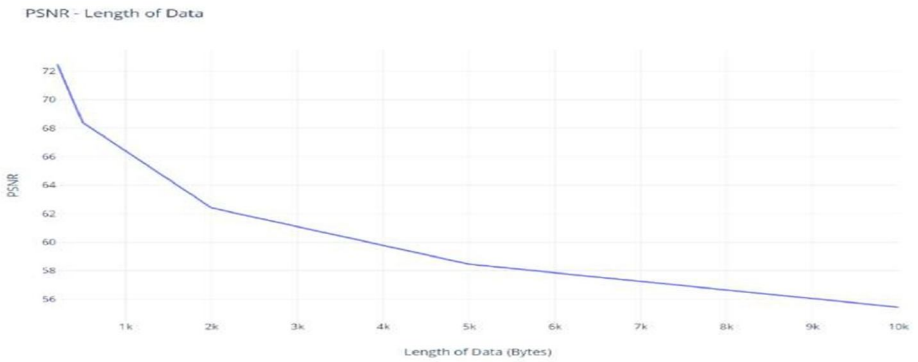


Fig 4.1.1 – Graph of PSNR/Length of Data

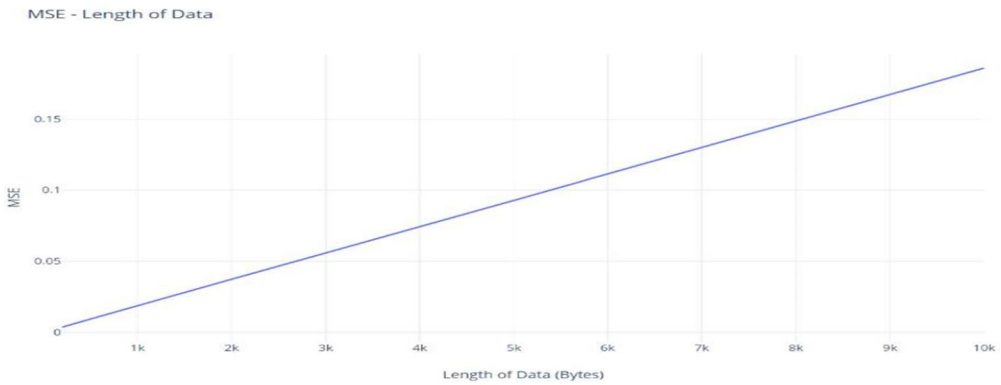


Fig 4.1.2 – Graph of MSE/Length of Data

The observed values of PSNR and MSE indicate that until 500 characters of data, the imperceptibility rate is very high. However, as the number of bits embedded keep increasing, the imperceptibility decreases and hence the algorithm is not very suitable for messages exceeding 10000 characters of data.

V. CONCLUSION AND FUTURE WORK

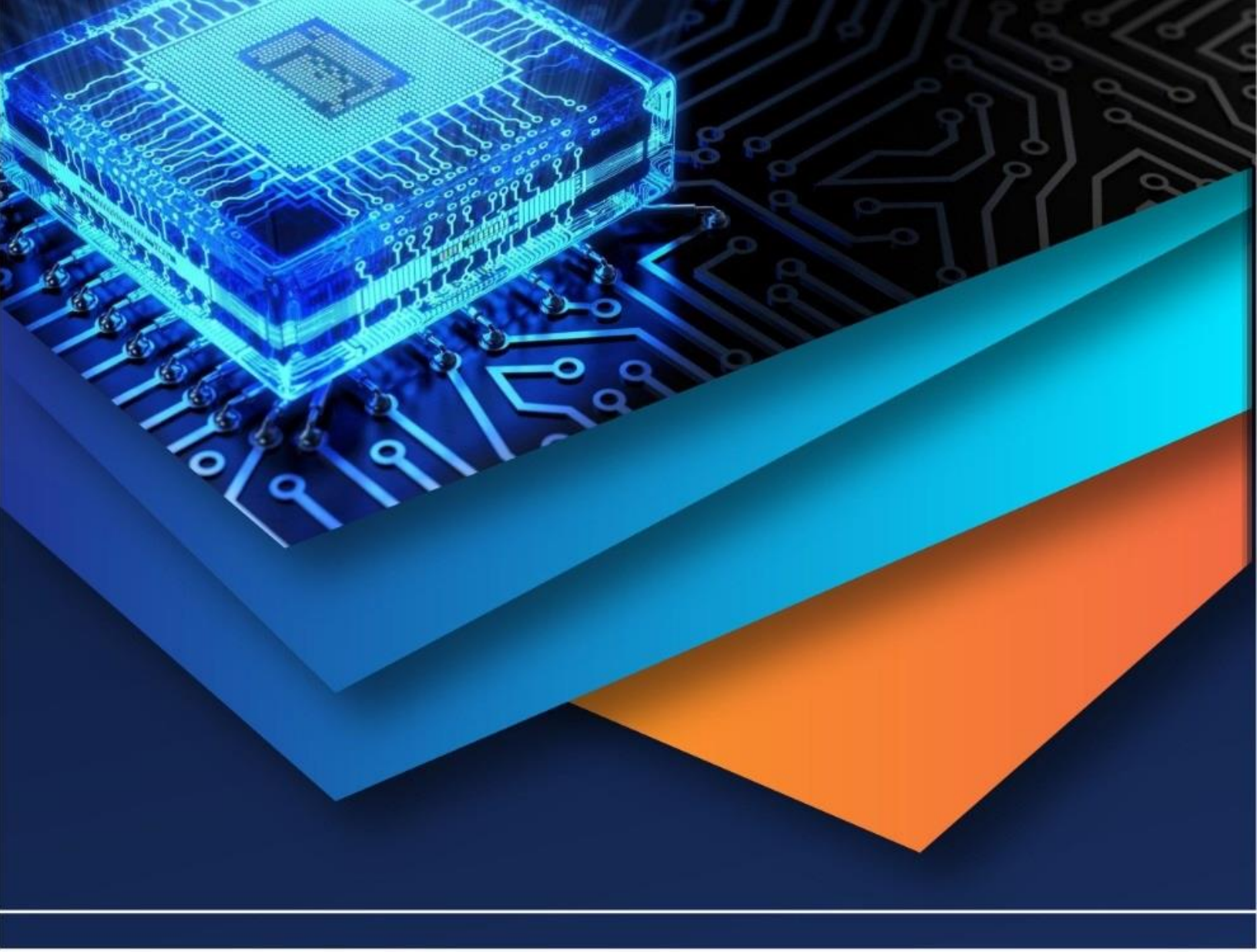
The study that has been provided thus far highlights the efficiency and synergy attained by combining cryptography with steganography. In particular, data protection and covert communication are greatly improved by this potent combination of security approaches. One of the main benefits is the retention of imperceptibility, which ensures that the concealed data stays essentially invisible to the human eye and concealed inside the host data. In addition, because of the encryption used, even if this composite data were to get up in the wrong hands, it would still provide a double layer of security. The RSA method was selected as the encryption technique for this particular project, demonstrating its dependability and durability in securing sensitive information. However, there are many exciting possibilities for investigation and improvement on the horizon for future study in this field. Comparing the implemented RSA algorithm against other cryptographic methods is one approach. This comparative analysis can be used to determine which algorithm is best for a certain application. Choosing the best algorithm can greatly improve the system's overall security and performance because each algorithm has specific strengths and drawbacks. For instance, when comparing several cryptographic methods, one may look at the speed, key length, and attack resistance.

The creation of a user-friendly interface is another intriguing possibility for future effort. This could be a mobile app or a web-based GUI made to enable users to connect conveniently and securely in the real world. Such a method would make secure communication available to non-technical people and spread the advantages of cryptography and steganography to a larger audience. This user-centric approach is vital because it fills the gap between effective encryption methods and everyday usability. Such an application has a significant potential impact. It let people, groups, and companies to transmit private information without worrying about it being intercepted. As a result, personal privacy is improved, and cybersecurity is strengthened in a time when cyberthreats are pervasive. Furthermore, being able to interact securely using an intuitive interface can have significant effects in industries like healthcare, banking, and law where secrecy is crucial.

In conclusion, combining steganography and encryption has proven to be a successful method for protecting data while keeping its secrecy. The RSA method is a good starting point for the research, but there are great chances to improve and develop these techniques in subsequent work. We can realize the full potential of secure and covert communication, making this technology useful to people and organizations around the world, by researching various cryptographic methods and creating user-friendly interfaces.

REFERENCES

[1] Laskar, S. A., & Hemachandran, K. (2012). High Capacity data hiding using LSB Steganography and Encryption. International Journal of Database Management Systems, 4(6), 57.
[2] Walia, E., Jain, P., & Navdeep, N. (2010). An analysis of LSB & DCT based steganography. Global Journal of Computer Science and Technology.
[3] Nisha, S., & Farik, M. (2017). Rsa public key cryptography algorithm–a review. International journal of scientific & technology research, 6(7), 187-191.
[4] Alese, B. K., Philemon, E. D., & Falaki, S. O. (2012). Comparative analysis of public-key encryption schemes. International Journal of Engineering and Technology, 2(9), 1552-1568.
[5] W. Ren and Z. Miao, "A Hybrid Encryption Algorithm Based on DES and RSA in Bluetooth Communication," 2010 Second International Conference on Modelling, Simulation and Visualization Methods, Sanya, China, 2010, pp. 221-225, doi: 10.1109/WMSVM.2010.48. (Placeholder1)
[6] Dixit, P., Gupta, A.K., Trivedi, M.C., Yadav, V.K. (2018). Traditional and Hybrid Encryption Techniques: A Survey. In: Perez, G., Mishra, K., Tiwari, S., Trivedi, M. (eds) Networking Communication and Data Knowledge Engineering. Lecture Notes on Data Engineering and Communications Technologies, vol 4. Springer, Singapore.
[7] S. Gupta and J. Sharma, "A hybrid encryption algorithm based on RSA and Diffie-Hellman," 2012 IEEE International Conference on Computational Intelligence and Computing Research, Coimbatore, India, 2012, pp. 1-4, doi: 10.1109/ICCIC.2012.6510190.
[8] Xin Zhou and Xiaofei Tang, "Research and implementation of RSA algorithm for encryption and decryption," Proceedings of 2011 6th International Forum on Strategic Technology, Harbin, Heilongjiang, 2011, pp. 1118-1121, doi: 10.1109/IFOST.2011.6021216.
[9] A. G. Devi, A. Thota, G. Nithya, S. Majji, A. Gopatoti and L. Dhavamani, "Advancement of Digital Image Steganography using Deep Convolutional Neural Networks," 2022 International Interdisciplinary Humanitarian Conference for Sustainability (IIHC), Bengaluru, India, 2022, pp. 250-254, doi: 10.1109/IIHC55949.2022.10060230.
[10] S. M. Masud Karim, M. S. Rahman and M. I. Hossain, "A new approach for LSB based image steganography using secret key," 14th International Conference on Computer and Information Technology (ICCIT 2011), Dhaka, Bangladesh, 2011, pp. 286-291, doi: 10.1109/ICCITechn.2011.6164800.
[11] J. Fridrich, M. Goljan and Rui Du, "Detecting LSB steganography in color, and gray-scale images," in IEEE MultiMedia, vol. 8, no. 4, pp. 22-28, Oct.-Dec. 2001, doi: 10.1109/93.959097.
[12] R. Chandramouli and N. Memon, "Analysis of LSB based image steganography techniques," Proceedings 2001 International Conference on Image Processing (Cat. No.01CH37205), Thessaloniki, Greece, 2001, pp. 1019-1022 vol.3, doi: 10.1109/ICIP.2001.958299.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY