Vol 3, Issue 10, 2020 Impact Factor:2.58 DOI: https://doi.org/10.31426/ijamsr.2020.3.10.3819

IJAMSR

International Journal of
Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

Advanced Image Security Using New Combined Approach of AES Cryptography and LSB Steganography

M. Loganathan
Assistant Professor, Department of Electronics and Communication Engineering, Thanthai Periyar Government Institute of Technology Vellore.
Email: logussr@gmail.com

R. Bharathiraja
Assistant Professor, Department of Electronics and Communication Engineering, Thanthai Periyar Government Institute of Technology Vellore.
Email: rajaecegce@gmail.com

A B S T R A C T

The implementation of a protected communication between two parties is becoming a problematic due to the possibility of attacks and other unintended fluctuations over an unsecured network. However, there are certain approaches called cryptography and steganography are commonly used to ensure security of secret data. These approaches are individually not appropriate for extensive security of various data. The secret image size is reduced using the discrete wavelet transform (DWT) in this work. Next, an advanced encryption standard (AES) approach is used to encrypt the information, resulting in a system of phases. The least significant bit (LSB) method is employed to hide the encrypted image. The results illustrate that the combined approach is achieved PSNR of 48.9 dB and SSIM of 0.93 for stego-image. This performance clearly demonstrates the combined approach is able to provide enhance the stego-image quality and structural similarity index.

Keywords: Discrete Wavelet Transform (DWT), Least Significant Bit (LSB), Cryptography and steganography, Advanced Encryption Standard (AES).

IJAMSR

International Journal of
Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

1. INTRODUCTION

Digital communication as a technique of transmitting information is now more common due to the Internet's fast development [1]. The most crucial problem with digital communication is the integrity and security of information transmitted across the internetwork connection. As a result, academics are working to find fresh ideas and methods for protecting sensitive information from malware and hacker exposure while it is transmitted via the internetwork [2]. In this work, we explore the most popular data security approaches, steganography, and cryptography, to give integrity and security to consumers in securing their access from unauthorized individuals.

Steganography is a technique for concealing sensitive information that uses a main picture but is incomprehensible to unauthorized individuals & hackers [3]. The essential authorities who know how to retrieve it have the sensitive information, but users cannot access it. The steganography may conceal sensitive data in the cover image using specific algorithms [4]. Everything represented as bits, including text, images, music, and video, can be secret messages. Transfer to the receiver starts with choosing the right channel. The decoder technology is employed with identical steganography for receiving original information from the sender after the hidden data have been inserted in the cover picture, also known as a steganographic [5]. Most significant bit (LSB) steganography methods are extensively utilized and regularly employed in various investigations. Images can be compressed to use less storage, quickly transport information, and pay less for internet traffic and storage hardware. We will therefore have a second layer of protection when we combine cryptography with hiding data.

Data can be concealed to stay private from unauthorized parties using cryptography [6]. Three alternative approaches are now employed, symmetric key, asymmetric key, and hashing [7]. Before, this system could only encrypt and decrypt transferred communications utilizing private keys. The actual text is the term used to describe the data that has to be concealed, while encryption is the technique used to do so. An "encryption key," the source to the process and the text, is often used to provide encryption. The recipient needs a decryption that employs an appropriate "decryption key" to decrypt encoded message and reveal the data [8]. Verification, confidentiality and secret, and integrity are three particular access control for every encryption method [9]. The most extensively used cryptographic algorithms in use today are DES [10], Rivest-Shamir-Adleman (RSA) [11], AES [12], Rivest Cipher 4 (RC4) [13], and others.

The process of compression involves lowering the amount of bits necessary to encode the information while maintaining or slightly lower (acceptable) accuracy [14]. Lossy compression and compression without loss are the 2 compression methods are offered [15]. Lossy compression states to approach that actual data such as images, drop few of its reality [16]. Several lossy compression techniques exist, including discrete cosine transforms (DCT), transform coding, chroma

IJAMSR

International Journal of
Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

subsampling, texture features and discrete wavelet transforms (DWT) [17]-[18]. Typically, medical imaging, artwork, and comics uses compression without losses. Predictive coding, Huffman coding, Run-length coding, Lempel Ziv Welch (LZW) and entropy coding [19]-[20] are a limited instances of compression procedures without losses. Thus, the DWT approach is employed to reduce images. It handles various image formats, including PNG, JPEG, and BMP. In terms of its picture library, DWT is reliable and efficient. It works well with data that is confined in time [21].

2. RELATED WORKS

A novel way of enclosing data inside the picture was recommended to improve security and efficiency. The DWT technique is used in this system to compress the hidden image, and AES algorithm is employed to encrypt the stored information. The LSB approach was used to conceal the encrypted information [21]. According to the analysis findings, when the tactics are used together, the quality of the steganography is preserved, performance is better by 44%. The approach secures the communication using the AES and columnar block ciphers, embeds it into the image using the 1-LSB approach, and then reverses the process to retrieve the information at the other end [22]. Hence, this approach maintains the image's architecture and adds a further degree of protection through powerful encryption algorithms.

Batch steganography protects information exchange from one end to the next. Frequently, the message can be encoded within the cover image using a password. The information is encrypted using the SHA-256 and AES hashing and encryption algorithms. Following the XOR operation, the encryption passwords have been employed [23]. Decrypting the information takes a long time without understanding the inputs and procedures employed; this protects against information stealing and potential cyber-attacks. The approach uses steganography and encryption for IoV and is believed. This technique's Efficient Algorithm for Secure Transmission (EAST) combines steganography and encryption [24]. This approach is compared to many algorithms, DES, G-DES, Standard LSB and AES. Outcomes for the recommended EAST approach are encouraging; compared to the latest research, it demonstrated superior speed of 0.86 ms, and PSNR of 78.58%.

Employing modern encryption standards, elliptic curves cryptography, and LSB steganography compared to new cube-based obfuscation will increase safety and memory for information stored in the cloud platform. Hybrid AES, ECC, LSB steganography [25], and Innovative Cube-Based Obfuscation Techniques are the 2 types considered. In addition to using less storage capacity, this method transforms the information into an unintelligible state that prevents attackers from identifying the image or stealing steganography images. According to the findings, cube-based obfuscation appears safe and takes up minimal storage capacity than hybrid ECC, LSB, and AES steganography.

IJAMSR

International Journal of
Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

DES and AES-based 128-bit crucial cross-breed method (CBA-128) is used to boost protection and employs steganography-based encryption to protect information [26]. At the same time, it is transmitted over the network. The model gives the data better protection to thwart unauthorized entry. The trials demonstrated effectiveness and efficiency in terms of duration and security settings.

To improve data security, four procedures were taken at both the source and recipient ends of the communication chain. First step, encrypt the image by using AES algorithm [27]. By using LSB-based picture steganography to conceal this combined text image and cover image, data security is increased. For safe information transfer from the sender end, the Steganography picture is separated and categorized. When the input data has been decrypted, several comparison indices, including PSNR, MS-SSIM, MSE and SSIM among the input and returned picture offer sufficient data integrity. A combined approach using the LSB and the RSA and Caesar Cipher methods is used in this framework. The findings from the test demonstrate the safety and excellent value of the cover data that won't be easily detached from the genuine image of the method [28].

The application of the AES-CBC and LSB combined steganographic cryptography approaches with image processing to search for less contrast regions where the encoded data will be placed [29]. This combined approach is established to direct a plaintext file hidden inside a BMP picture, making any changes to the image invisible to the human eye and undetectable by steganographic analysis. It's discovered as a consequence that the fusion method used has three levels of protection over plaintext that has been encoded and concealed in a picture, making it challenging to compromise the security of the data transferred in a stego-image. The method emphasizes the LSB matching steganography approach. Before using the steganography approach to secure two-layer protection of private communication [30], the AES technology is employed for increased safety. Moreover, the enhanced LSB steganography method supports mosaic pictures well. Stego-image provided great PSNR values than other ways using a superior version of LSB when the concealed text was incorporated into the mosaic image. The PSNR value of the recommended method, which has a maximum capacity of 32 bytes, is 85.65 dB compared to other spatial domain techniques.

3. PROPOSED METHODOLOGY

We provide a hybrid approach to blend a hidden picture into another. This system uses three algorithms to increase data security and efficiency: the DWT compression technique, the AES cryptography, and the LSB steganography approaches. The combined architecture of the designed approach is shown in Figure 1 and 2. The two critical stages of the proposed approach are implantation and extraction. The tasks that need to be finished to protect and hide the unseen image confidential the cover image is included in the implantation phase. The sender uses the DWT technique to compress the hidden image and the AES algorithm to encrypt the trampled image to create ciphered bits, which are then implanted

IJAMSR

International Journal of
Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

into the cover image using the LSB method. Stego-images is delivered to the receiver over the cyberspace. The encryption image will be taken since the stego-image during extraction to obtain the hidden picture. Afterward, employing the same key as during encryption, the computed data is decoded by applying the AES. The DWT procedure is then applied to decompress the hidden picture.

3.1 Discrete wavelet transform

The wavelets are separately experimented in DWT. A DWT's primary advantage is the periodic resolution that its Fourier transforms enable [31]. DWT gathers location and frequency data over time. Wavelets are local signals having uneven shapes, some different arrangements, and the mean value is 0. Wavelets oscillate up and down with the axis and integrate to zero. Several wavelets have an orthogonal property that is suitable for a compact signal presentation and guarantees that data is not heavily represented [15]. A wavelet transform divides the signal into scaled and shifted copies of the real wavelets or components. The wavelet coefficients are decreased until the decomposition is finished to eliminate some details.

3.2 Advanced encryption standard

The National Institute of Standards and Technology (NIST) has picked the symmetric block cipher, Rijndael as the AES. The data encoding approach is modified with this method (DES). AES employs a single key that might be 128, 192, or 256 bits long as part of the encryption [32]. AES is an asymmetric encryption algorithm since it uses the same encryption and decryption key. Asymmetric encryption techniques, in contrast, employ two distinct keys: public and private. A binary data string used for encoding is all that an encryption key is [33]. While utilizing the identical encryption key to encode and decode the data, it is crucial to keep it secret and to choose keys that are challenging to decipher. Programs used for this specific job can generate several keys, which can also be derived from the passphrase. A single password should never be used as the encryption key in a good encryption scheme.

3.3 Least significant bit steganography

The commonly used LSB stenographic algorithm embeds the hidden picture inside of an image cover. Binary conversion is possible for the cover image and secret image pixels. One bit of the hidden image replaces the LSB of the cover image. A stego-image is the product of concealment when the hidden picture is included in the cover image. Mathematical explanations for joint LSB operations are given in [34].

This implementation aims to further this crucial area of scholarly research by investigating the combined security model and testing of various situations. Figures 1 and 2 shows the recommended model is realized. The security model which guides the user complete queries concerning the approach and the user should select such as Source block or destination block.

International Journal of
Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

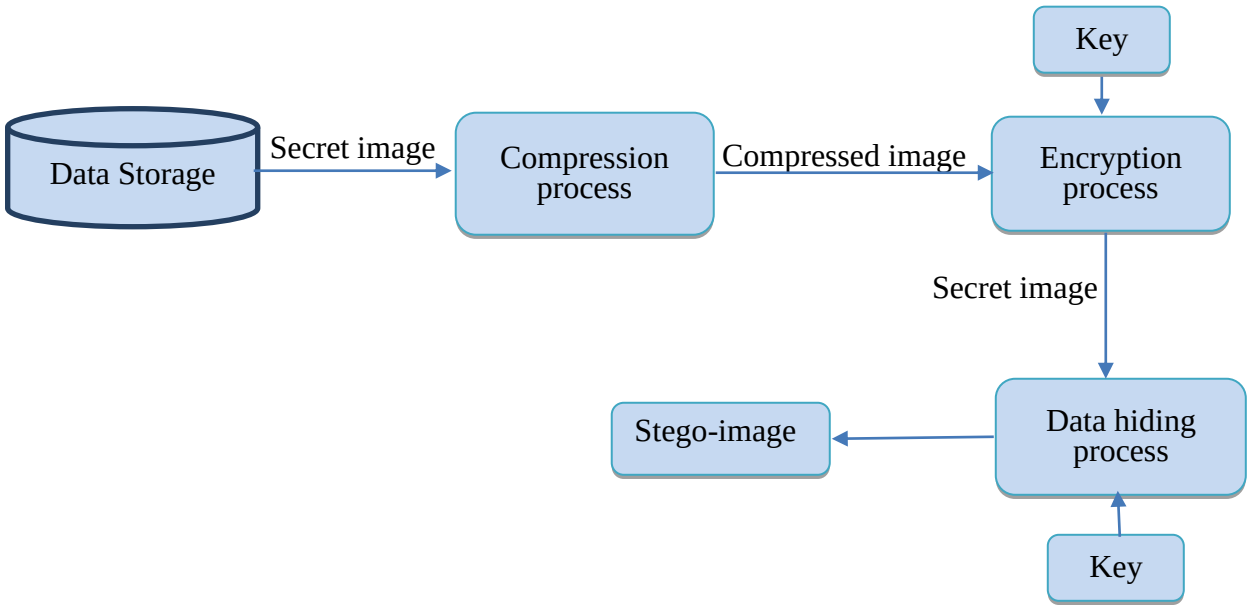

Figure 1: Sender side

The module executes the subsequent process if Sender Side is chosen.

Stage 1: choose a cover image from data storage.

Stage 2: select a hidden image as our input image.

Stage 3: By selecting the "compress picture (DWT)", you may reduce the size of secret image using the DWT technique as the first layer. You can then examine the reduced image in the reduced image size.

Stage 4: To implement the second layer, choose the "Encrypt picture (AES)", then type the hidden key to encode the hidden information, which has a length of 128 bits. The application then turns the reduce image size into a binary array byte to be encoded using the AES technique.

Step 5: In the last layer of the proposed approach, select "Steganography (LSB)" to insert the hidden image in the case/cover image. The cover image pixels must be converted into binary format for this layer. The RGB cover image's pixels each correspond to an 8-bit byte. As an outcome, with our initial system's LSB image-based steganography, we were able to conceal 1 bits of hidden information in each pixel.

International Journal of
Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

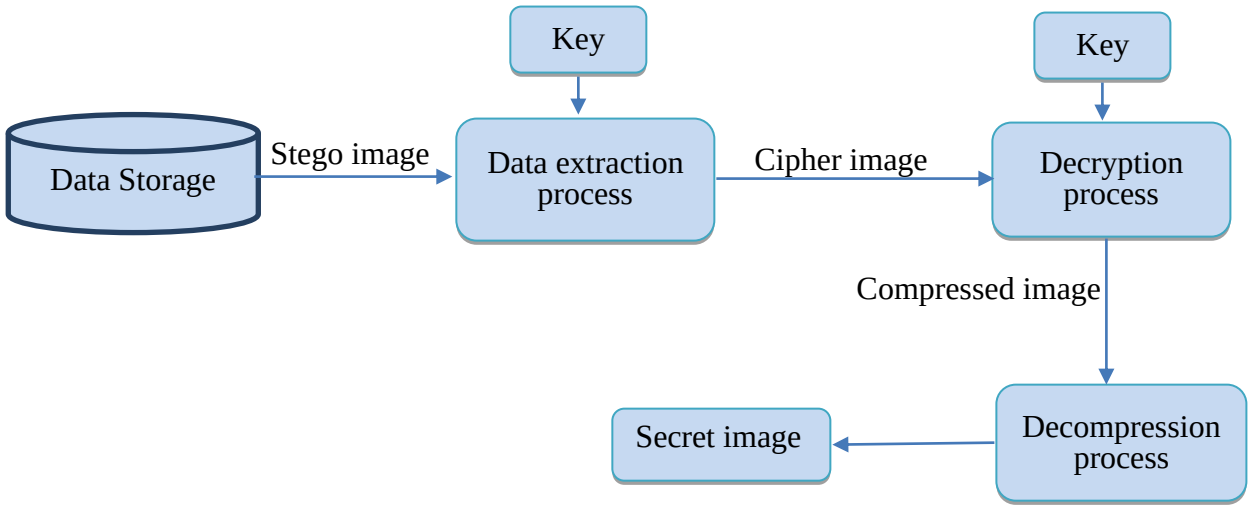

Figure 2: Receiver side

The module executes the subsequent process if Receiver Side is chosen.

Stage 1: chosse a stego-image.

Stage 2: To get the encoded information from the concealed image and illustrate it in the encoded image.

Stage 3: With the similar hidden key in the encoding procedure, assessment the reduced image.

Stage 4: To attain the hidden image, view the input image in the hidden image region.

4. RESULT AND DISCUSSION

The confidential image is compressed and encrypted in the proposed approach before being hidden in cover images, as said, to be examined and evaluated. To further explain this, we selected ten cover images of various sizes and, following extensive tests, evaluated the performance data.

A method for assessing how similar two pictures are is called structural index similarity (SSIM). The standard evaluates an image's quality compared to a distortion-free input image. A reference, the presenter image is utilized while the stego-image is being examined, regarding stego-image in data. The presenter image is regarded as the input image, and the stego- image is the image being analyzed.

$$SSIM\ (h,S) = \frac{(2\mu_h\mu_s + b1)(2\sigma hs + b2)}{(\mu_h^2 + \mu_s^2 + b1)(\sigma_h^2 + \sigma_s^2 + b2)}$$

Maintaining the divide Indicating the covariance and average of the variables, the denominator is made weak by the variables b1 and b2, respectively.

IJAMSR

International Journal of
Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

The PSNR is the ratio of the determined signal to the total noise it is subjected to.

$$PSNR = 10.Log10 \frac{max^2}{MSE}$$

To determine the quality differential between the cover picture and the steganography, the PSNR is utilized. The PSNR is better if the PSNR is higher. The performance of the suggested strategy to conceal hidden pictures was assessed using the performance metrics PSNR and SSIM. The evaluation criteria for applying this proposed strategy to the ten images are shown in Table 1. Figures 3 and 4 show the results from Table 1 visually. According to the performance evaluation for the approach in Figure 4, the average PSNR is 48.9 dB, which is close to other methods in most cases. According to the average value, the stego-image quality is good. The visual quality distortion in the stego-image is often problematic for human eyes to detect if the PSNR value exceeds 45 dB. We can validate using LSB that the high PSNR values indicate a well-hidden image with little noise influence throughout the operation. The SSIM parameters for the steg-image are likewise evaluated using the proposed methodology. The average SSIM value was discovered to be 0.93, as shown in Figure 3. High SSIM values, in other words, show that the approach only little altered the stego-images.

Table 1. findings of performance metrics using SSIM and PSNR

Stego-Image	SSIM	PSNR
Image1	0.9318	48.391
Image2	0.9265	46.802
Image3	0.9311	48.147
Image4	0.9399	44.677
Image5	0.9176	51.204
Image6	0.9451	47.118
Image7	0.9188	47.355
Image8	0.9452	50.038
Image9	0.9369	52.899
Image10	0.9244	49.441

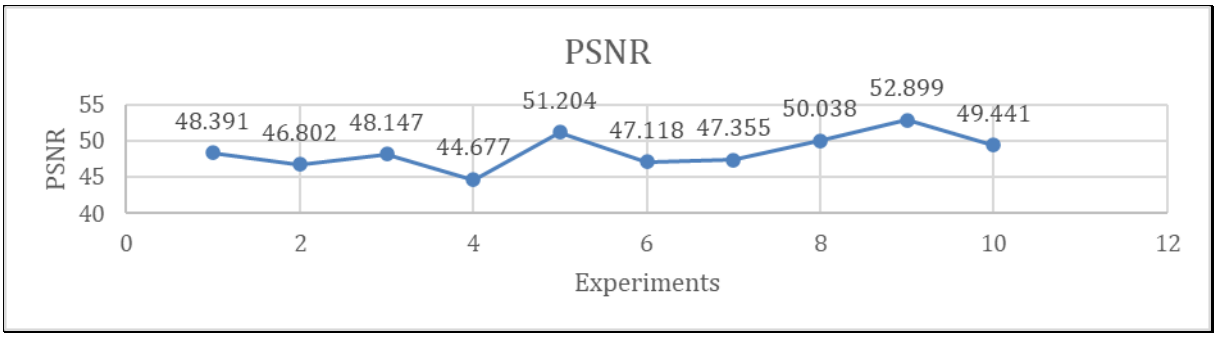

Figure 3. The SSIM value of stego-image

International Journal of
Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

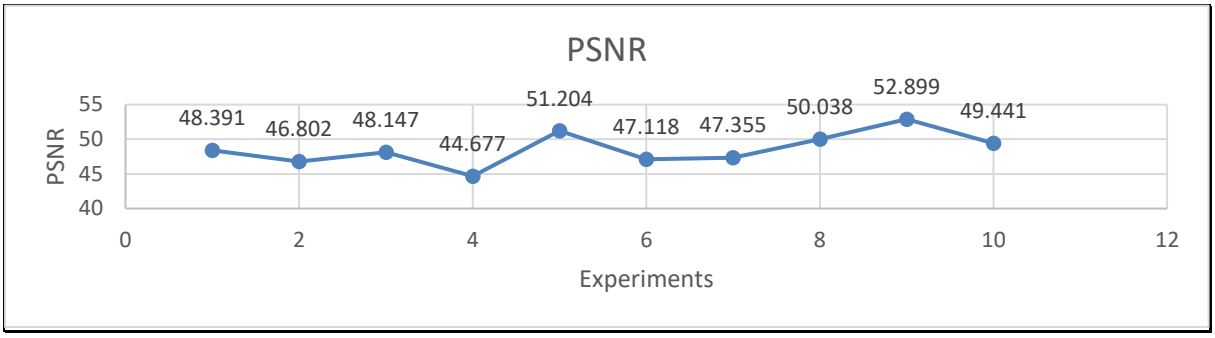

Figure 4. The PSNR value of stego-image

According to our work, combining approach steganography, encryption, and compression techniques can increase system security and evaluation greater than using each approach alone.

5. CONCLUSION

For high security and capacity, a combined security approach that hiding secret image inside another image. This combined approach has three consecutive process such as compression, cryptography and steganography. In compression process, DWT approach is use to diminish the hidden image size. Then, an AES technique is used to confirm hidden security of image and use the LSB approach to hide secret image within the case/cover image. The experiment outcomes depict the mean PSNR 48.9 dB and average SSIM 0.93 with good quality of stego-image. This proves the combined approach improves the data security and its performance due to its three layers of security.

REFERENCES

1) Mohanty, S. P., Choppali, U., & Kougianos, E. (2016). Everything you wanted to know about smart cities: The Internet of things is the backbone. *IEEE Consumer Electronics Magazine*, *5*(3), 60-70.
2) Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, *80*(5), 973-993.
3) Jayaram, P., Ranganatha, H. R., & Anupama, H. S. (2011). Information hiding using audio steganography–a survey. *The International Journal of Multimedia & Its Applications (IJMA) Vol*, *3*, 86-96.
4) Umamaheswari, M., Sivasubramanian, S., & Pandiarajan, S. (2010). Analysis of different steganographic algorithms for secured data hiding. *IJCSNS International Journal of Computer Science and Network Security*, *10*(8), 154-160.
5) Maiti, C., Baksi, D., Zamider, I., Gorai, P., & Kisku, D. R. (2011). Data hiding in images using some efficient steganography techniques. In *Signal Processing, Image Processing and Pattern Recognition: International Conference, SIP 2011, Held as Part of the Future Generation Information Technology Conference FGIT 2011, in Conjunction with GDC 2011, Jeju*

IJAMSR

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

Island, Korea, December 8-10, 2011. Proceedings (pp. 195-203). Springer Berlin Heidelberg.

6) Saleh, M. E., Aly, A. A., & Omara, F. A. (2016). Data security using cryptography and steganography techniques. *International Journal of Advanced Computer Science and Applications*, *7*(6).
7) Bokhari, M. U., & Shallal, Q. M. (2016). A review on symmetric key encryption techniques in cryptography. *International journal of computer applications*, *147*(10).
8) Goshwe, N. Y. (2013). Data encryption and decryption using RSA algorithm in a network environment. *International Journal of Computer Science and Network Security (IJCSNS)*, *13*(7), 9.
9) Ren, K., Lou, W., Kim, K., & Deng, R. (2006). A novel privacy preserving authentication and access control scheme for pervasive computing environments. *IEEE Transactions on Vehicular technology*, *55*(4), 1373-1384.
10) Singh, G. (2013). A study of encryption algorithms (RSA, DES, 3DES and AES) for information security. *International Journal of Computer Applications*, *67*(19).
11) Manjula, Y., & Shivakumar, K. B. (2016, March). Enhanced secure image steganography using double encryption algorithms. In *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)* (pp. 705-708). IEEE.
12) Schmittner, M., Asadi, A., & Hollick, M. (2017, June). SEMUD: Secure multi-hop device-to-device communication for 5G public safety networks. In *2017 IFIP networking conference (IFIP Networking) and workshops* (pp. 1-9). IEEE.
13) Luntovskyy, A., Spillner, J., Luntovskyy, A., & Spillner, J. (2017). Architectural transformations in distributed systems. *Architectural Transformations in Network Services and Distributed Systems*, 13-44.
14) Toderici, G., O'Malley, S. M., Hwang, S. J., Vincent, D., Minnen, D., Baluja, S., ... & Sukthankar, R. (2015). Variable rate image compression with recurrent neural networks. *arXiv preprint arXiv:1511.06085*.
15) Kavitha, P. (2016). A survey on lossless and lossy data compression methods. *International Journal of Computer Science & Engineering Technology*, *7*(03), 110-114.
16) Sharma, M., & Gandhi, S. (2012). Compression and encryption: An integrated approach. *Int. J. Eng. Res. Technol*, *1*(5), 1-7.
17) Mathey, R., & Avadhani, P. S. An Multi Resolution Using Discrete Wavelet Transforms and Fractals Transforms.
18) Vrindavanam, J., Chandran, S., & Mahanti, G. K. (2012, March). A survey of image compression methods. In *Proceedings on international conference and workshop on emerging trends in technology* (pp. 12-17).
19) Bandyopadhyay, S. K., Paul, T. U., & Raychoudhury, A. (2011). Image compression using approximate matching and run length. *International Journal of advanced Computer science and applications*, *2*(6).
20) Kaur, R., & Kaur, M. (2017). A Survey of Medical Image Compression Techniques. *International Journal of Advanced Research in Computer Science*, *8*(4).

IJAMSR

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

21) Brar, S. S., & Brar, A. (2016). Double layer image security system using encryption and steganography. *International Journal of Computer Network and Information Security*, *8*(3), 27.

22) Bansod, S. P., Mane, V. M., & Ragha, R. (2012, October). Modified BPCS steganography using Hybrid cryptography for improving data embedding capacity. In *2012 International Conference on Communication, Information & Computing Technology (ICCICT)* (pp. 1-6). IEEE.

23) Saini, J. K., & Verma, H. K. (2013, December). A hybrid approach for image security by combining encryption and steganography. In *2013 IEEE second international conference on image information processing (ICIIP-2013)* (pp. 607-611). IEEE.

24) Wajgade, V. M., & Kumar, D. S. (2013). Enhancing data security using video steganography. *International Journal of Emerging Technology and Advanced Engineering*, *3*(4), 549-552.

25) Chawhan, A. T., Manjula, Y., Shivakumar, K. B., & Kurian, M. Z. (2015). Enhanced LSB image steganography using Hybrid EncryptionLZW Compression and Knight Tour Algorithm. *International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)*, *14*(2).

26) Riasat, R., Bajwa, I. S., & Ali, M. Z. (2011, July). A hash-based approach for colour image steganography. In *International Conference on Computer Networks and Information Technology* (pp. 303-307). Ieee.

27) Mandge, T., & Choudhary, V. (2013, February). A DNA encryption technique based on matrix manipulation and secure key generation scheme. In *2013 International Conference on Information Communication and Embedded Systems (ICICES)* (pp. 47-52). IEEE.

28) Kaur, M., & Randhawa, A. P. R. K. (2017). Hybrid Approach For Improving Data Security And Size Reduction In Image Steganography. *International Research Journal of Engineering and Technology (IRJET)*, *4*(6), 2845-2850.

29) Tuncer, S. (2016). Information Encryption and Hiding into an Image by Steganography Methods to Improve Data Security. *Journal of new results in science*, *5*, 170-177.

30) Shawkat, S. A. (2007). Enhancing steganography techniques in digital images. *Faculty of Computers and Information, Mansoura University Egypt-2016*.

31) Dong, J., & Li, J. (2016). A robust zero-watermarking algorithm for encrypted medical images in the DWT-DFT encrypted domain. In *Innovation in Medicine and Healthcare 2016 4* (pp. 197-208). Springer International Publishing.

32) Janapriya, B. (2017). Video Steganography Schema based on AES Algorithm and 2D Compressive Sensing. *Image*, *3*, 4.

33) Blackledge, J., Bezobrazov, S., & Tobin, P. (2015, July). Cryptography using artificial intelligence. In *2015 International Joint Conference on Neural Networks (IJCNN)* (pp. 1-6). IEEE.

34) Zhang, T., Li, W., Zhang, Y., & Ping, X. (2010, April). Detection of LSB matching steganography based on distribution of pixel differences in natural images. In *2010 international conference on image analysis and signal processing* (pp. 548-552). IEEE.