ISSN No. 0976-5697

Volume 8, No. 5, May – June 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Enhancement of Security in Cloud Computing using Steganography

Ataussamad
Dept. of Computer Science and Eng.
MMM university of Technology
Gorakhpur, Uttar Pradesh, India

Dr. Shiva Prakash
Dept. of Computer Science and Eng.
MMM university of Technology
Gorakhpur, Uttar Pradesh, India

Abstract: Cloud computing is a prominent method of accessing shared and dynamically configurable resources through network on demand. It is excessively used by mobile applications to offload data over the network to the cloud. There is a prominent need of security on the cloud data as it is stored at mobile locations, so we have proposed an approach to provide a double security to the cloud data using the digital image steganography technique as well as the cryptography technique. In this work we tried to secure the cloud transmission by means of Optimized Blowfish algorithm for the encryption of secret message. In the next step steganography method is used where we have employed the Dynamic Circular Queue in the cover image to embed the encrypted message bits into circular blocks of the cover image which makes it more secure than simple LSB substitution method. When the receiver needs to obtain the information he needs to select the Cover image which is than unhidden using the same circular queue substitution. Authorized receiver will determine the right plain text using private key in Blowfish de-cypherment. Performance analysis is evaluated by using MSE, PSNR values. Results are higher as compared with several of existing algorithms of image steganography.

Keywords: Steganography, DCQ, PSNR, MSE.

I. INTRODUCTION

Steganography is a practical technique whereby encoded data is hidden intimate a transporter file in command to achieve the goal that the modification made in visibility of the resultant file might not be obviously noticeable to typical human eye. In most similar way with in cryptography where the personal data is encoded generating a key, anyone can hint that message communication is establishing regardless of the fact that deprived of the key attacker cannot access the data. Whereas, in steganography technique it is very challenging to trace that some undisclosed or confidential data is in transport state [1]. What is further, on the off way that anyone might not know that there is some confidential data; the individual won't attempt to untangle the data. There are 3 types of methods to accomplish Steganography [2] using three types of conveyors i.e. steganography in the form of pictures, steganography in the Audio fie and steganography in the Video file. The concept of the key behind steganography is that the intimate data to be dispersed is not traceable to the unintentional eye. The core difference amongst the two techniques: steganography and cryptography is that in the case of cryptography it is easily known that a message has been encrypted, but due to lack of the proper key it is unable to be decoded. In steganography, there is not much transformation as the message is not self-visible, and most people or attacker would not be able to detect the presence of the private message. When combined, both of these two techniques can provide enhanced two levels of security. Computer programming language exist which can encrypt a confidential message using cryptography, as well as hide the encryption inside an image using LSB encoding insertion or other types of steganography.

II. LITERATURE REVIEW

In comparative study of our dissertation work we have found the similarities and differences between the various securities algorithms present in the literature survey. We have done our comparative study on the basis of certain parameters given below in the table using Blowfish Algorithm and Optimized Blowfish [3] Cipher block. Blowfish [4] is a symmetric key algorithm which could be used as a casual substitution for DES or IDEA. It takes a variable-length key, from 32 bits to 448 bits, making it perfect for together of domestic as well as commercial usage. Blowfish is unpatented, has cost free license and is available open source for all uses. Blowfish consumes very less time in encryption/decryption and scored highest entropy which is also called 'randomness of information' in comparison to other algorithms like RSA and DES. Each of the encryption methods has its own particular solid and frail focuses. With a specific end goal to apply a reasonable cryptography algorithm to an application, we ought to have learning in regards to execution, quality and shortcoming of the algorithms.

The author Christina L, Joe Irudayaraj V S in 2015 [5] proposed an optimized Blowfish algorithm for steganography. Optimized Blowfish is a 64 bit block cipher with a 448 bit key length. It is a Feistel network consisting of 16 rounds. The relative strength of the encryption algorithm is based on key length. Optimized Blowfish algorithm keeps two sub key arrays: P-array and two 32 bit S-boxes. This algorithm is divided into three main parts: sub keys generation, S-Box preparation and Encryption. Description of optimized Blowfish Encryption Algorithm is elaborated below in three phases. In this algorithm the S-Box values are first encrypted and then the four S-Box are combined into two S-Box therefore reducing the memory size as well as enhancing its performance. In the table below most of the Parameters are defined on the basic of which we have done the comparative study of the two algorithms.

In [6], the author has revealed nested imprints which are implanted in a main image and these imprints are to be encrypted before embed using the blowfish algorithm. Consequences show a notable embedded capacity and security in the watermarks. Trials are done to review the act of blowfish algorithm by aggregate the file size as well as the key length. The equations resulting from the results are reserved for evaluating future enactments.

In Honeyman P.,Provos N. in 2003[7] highlighted on this topic as steganography is an art & science of encapsulating communication; a steganography system thus hides the encrypted content in unmark able cover medium so as no eavesdropper's can suspect it. Mostly, the secret data-hiding process in a steganography infrastructure initiates by identifying a cover media inordinate bits (those one which could be altered without disrupting that mediums integrity) the hiding process evolves a stego media by re-placing these inordinate bits with secret data from the encapsulated message. The method proposed here provides two level of security paradigm which is much better than previous methods. Normally, the confidential-data is encapsulated using RSA public-key cryptographic algorithm, and the encapsulated data is hidden with the LSB's of cover media image implementing circular and round queue method, and hence the strength of the steganography algorithm could be enhanced using the cryptography algorithm. In this method encapsulating the data into the LSB's of the cover image also didn't decrease the image quality much.

In the article the author Tanmay Bhattacharya et. al.'s [8] used a session oriented encryption as well as cross fold transportation algorithm for embedding purpose. First the secret records is transformed into binary method preferably text data and the cross fold transportation is performed on it. This binary conversion yields a genetically yielded session key and embed inside the host image data. For extraction purpose both the Stego and the original image is sent along with the session key. There are so many procedures which have been used to hide the vast variety of multimedia private data inside various multimedia files.

Saiful Islam, Mangat R Modi and Phalguni Gupta [9], in this paper proposes a novel steganography procedure, where edges in the cover picture have been utilized to hide messages. The measure of the information assumes an exceptionally crucial part in the determination of edges i.e. as the information estimate builds we move towards the weaker edges to implant the information. Numerous exploratory outcomes recommend this proposed procedure works better in any event as indicated by the best in class steganography methods yet it additionally yields higher implanting limit.

The modified version of the blowfish proposed by the author [10] which optimized blowfish algorithm further yields better result that the original blowfish algorithm, thus by reducing the number of S-Box used from four to two and the number of functions were also minimized in the optimized blowfish only XOR function is used rather than using both XOR and modulo function. On the basis of this comparative survey we reach to the conclusion that Optimized Blowfish will yield better results for encryption and it will make the steganographic process more effective and secured.

The Author Venkata Abhiram.Met.al's[11] gives us an approach of randomised technique which uses the approach of using RGB values so as to enhance the imperceptibility value of coloured images. In the three channels available which are GREEN, BLUE, RED the Least Significant Bit (LSB) of any one of the channels can be used as a pointers to obtain the encoding capacity of the two other channels. If we use the randomising technique, LSB's of any of the one channels can be used as a pointer to yield how to hide the data in the other two remaining channels. If we found the last two digits to be Zero-Zero than there might be no hidden data present, if the value is Zero-One than the data is embedded in Channel two only, if the value is One-Zero data is embedded in Channel one only and if the value is One-One than the data is embedded in all two channels present. The author tells us about the three methodologies used which are 1. RED is always used as a Default pointer.2. User ca select or adopt any channel as a pointer.3. The Pointers are chosen depending upon a cyclic sequencer and data gets embed. Images were collected and all the same sized data is embedded applying all the methods. Studying the values of the histogram and MSE and PSNR values the third method which is randomised approach yields better performance and accuracy with the availability of enhanced embedded capacities.

The author G Sahoo et al. [12] recommends the use of the movie clip as a file carrier to enhance the carrying capacity of the secret data. This method works on the replacement concept in which all of the non-sensitive pixel as well as some of the parts associated with the sensitive pixel is substituted with the secret data. An example of the movie clip which is temporal sequence of the 2D sample of the visible field with each sample as a frame of the movie. The movie frame parts can be divided in to the static and moving parts. Both the static as well as dynamic parts can be obtained by the Pixel Level Analysis, Colour Histogram or the other methods and all are stored in a Static as well as dynamic buffer. In static part embed process uses one pixel to store the 3 characters by using this formula xaj = a+ (j-1)*d where a is the initial location, j is the character of the private message and d signifies the distance between the 2 embed pixels. In dynamic part the embedding Most Significant Bit (MSB) is used. We use a different Steganography key for the Dynamic part. The major advantage is the hiding capacity in this method.

The author Nag et al. [13] in 2011 proposed a very novel approach in steganography which was based on the affinitive encryption algorithm and encapsulates the secret data at the first LSB position in order to give advice for a solid security and insignificant quality of the secret data. The novel approach could be easily understood by his article.

The Author Lenka and Swain [14] in 2015proposed a new start of the stenographic technique which was based on the LSB array. One from the four arrays was selected and on the parameter of the length of the private message. The other words from the same data was chosen and mapped onto the array, where the max of the matches found and the obscured data indices are noted down for the encryption in the Steganography technique.

In the year 2016 the author Mamta Jain and Saroj Kumar Lenka[15] proposed an approach where the author combined the use of RSA cryptosystem for encryption/ decryption and for steganography purpose he used the Adaptive dynamic circular Queue instead of LSB substitution to store the data into the image bits which yields better values in terms of MSE and PSNR and the distortion is also less, the images output were clearly visible to Human Vision System.

III. PROPOSED WORK

We assume the system as a cloud environment here we have used the Net Beans framework for the implementation of our coding work. The coding is done in JAVA programming language we have assumed three Screen windows to be Our User site, Server site and the output of the implementation is shown on the output window. We have used the Windows 10 operating system with minimum 1 GB of RAM. We have used MySQL server to get it linked it with our IDE. We have given an input text to our User Screen Window and saved it to a location on the system and then we will encrypt the text by selection of an image as a cover medium which is saved to a location on the system, in the next phase we will retrieve the secret text from the cover image where we have hidden it.

To enhance the level of security we have proposed an approach where we will first select an image to be used as cover image and the secret message which is to be embedded into the image selected, we now convert the secret message into encrypted message by the means of optimized Blowfish algorithm for embedding, now the obtained cypher text will be divided into blocks each block having 7 bits rather than 8 bits because it is the property of full circular queue in which one slot is empty which is its property. Now the cover image will be divided into except for some fixed locations into i.e. 16 image blocks each image blocks having the same no. of pixels, now organize first byte of all the sixteen image blocks into one circular queue, second bytes of all sixteen image block into second queue and so on. After the dynamic procedure is adapted we will subtract all the integer number values of first byte data and from all blocks by 255.Now for dynamic selection to proceed for the embedding we take the starting 4 bits of first bytes of the particular selected data and so on by adapting this procedure until all the bits are embedded.

Our main objective is to minimize the PSNR value in order to maintain the quality of the image file in terms of less distortion and less susceptible to HVS which is to be used as the cover medium so that no attacker can guess that there is some data hidden into the image.

Proposed Methodology

Encryption side

Step1: Using edge detection method to obtain the output edge image B from the image G.

Step 2: Applying Blow Fish encryption algorithm to get the encrypted secret image and divide the output edge image B into set of blocks, for each block comprising of n-pixels. We used P1 pixel to store output status of others pixels. If it is an edged pixel then the position of each pixel “Pi”, defined as ‘1’ otherwise it is ‘0’ in case of non-edged pixel. The position of pixel from P2 to ‘Pn’ is kept inside P1 by LSB replacement operation.

Step 3: For non-edge pixel inside a block we embedded ‘y’ message bits XOR with ‘y’ MSB’s of pixels by LSB substitution method.

Step 4: In an edge pixel inside a block, embedding ‘x’ bit of message is XOR with “x” MSB’s of a pixel by LSB substitution method.

Decryption side

Step1: Similar to divide operation performed in the previous procedure. Applying Optimized Blow Fish decryption algorithm and extract the original image and divide the stegano image into ‘n’ pixel block.

Step2: It is based on the (‘n’ - 1) LSB in a pixel ‘P1’, we obtained the position of the remained pixels starting from‘P2’ to ‘Pn ’. Now with this status value, we could identify 2 categories matching to the non-edged pixel category as well as edged pixels category.

Step3: From a non-edged pixel, established on the values of ‘y’ which is used in the embedding process we extracted the ‘y’ LSB of the pixels and ‘XOR ’with the ‘y’ MSB of a pixel to yield the original bit of the message.

Step4: In this step from edged pixel, which is based on values of ‘x’ produced randomly, yield ‘x’ LSB of a pixel and ‘XOR’ with the ‘x’ MSB’s of a pixel to complete part of the message. Values of ‘x’ produced will be same for pixels in extraction and embedding.

3.1 Algorithm

Sender side Algorithm: Implement this task is as follows:

```
Sender-(input as text)
{
If (text = = text)
{
Initialize the file request
File output = Encrypt text (text-input, file- output)
Pseudo-code of Encryption
 Divide the 64 bit input data into two 32-bit halves (left and right): xL and xR
fori=0 to16
xL is XOR with P[i].
Find F(xL)
F (xL) is XOR with xR.
Interchange xL and xR.
xR is XOR with P[16].
xL is XOR with P[17].
Finally combine xL and xR.
Cover image = Embed the cipher text into image file with using DCQ substitution method.
Request_send_the file
}
else
}
Message (“Application denied due to non-text data”)
}
```

Receiver Side

```
Receiver (input as cover image)
{
File = Extract the cipher text from cover image with using same DCQ method
Decryption (input text, file output)
Pseudo-code of Decryption
Step 1: Divide the 64 bit input data into two 32-bit halves (left and right): xL and xR
Step 2: for i=17 to1
xL is XOR with P[i].
Find F(xL)
F(xL) is XOR with xR.
Interchange xL and xR.
xR is XOR with P[1].
xL is XOR with P[0].
Finally combine xL and xR.
Download output file
}
```

IV. Result and Analysis

We have employed our concept by means of the NetBeans framework and Java language for coding. Since our main task is to enhance the security and privacy of the data as well make it less prone to attackers we have done two phase of security in first phase we will try to encrypt the private data and in the next phase we will hide the data by substituting it with the LSB of the circular Queue. We have coded in java and assumed a cloud environment in which we created few modules for our proposed work to take input of the secret message and give output at the output end as well as intermediate steps will provide the security by encryption and LSB substitution. So we have implemented the Snapshots in next section and comparison between existing work and our proposed work is shown in a graphical representation in upcoming section.

4.1 Calculation of (Peak Signal to Noise Ratio):

The PSNR square figures the pinnacle flag to-commotion proportion, in decibels, between two pictures. This proportion is frequently utilized as a quality estimation between the first and a packed picture. The higher the PSNR, the better the nature of the compacted, or remade picture. We can calculate by using this formula

$$\mathbf{PSNR=10}\ \log_{10}\left(\frac{R^2}{MSE}\right)$$

Where R is the maximum fluctuation in the input image data type.

4.2 Calculation of (Mean Square Error):

The Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR) are the two important measurements used to think about picture pressure quality. The MSE speaks to the total squared large difference between the compacted and the first picture, while PSNR speaks to a measure of the pinnacle mistake. The lower the estimation of MSE, the lower the mistake.

To process the PSNR, the piece first computes the mean-squared blunder utilizing the accompanying condition:

$$\mathbf{MSE=}\ \sum_{M,N}\frac{[I_1(m,n)-I_2(m,n)]^2}{M*N}$$

Where MxN are array size with I_1 as Original frame copy I_2 as Stegano frame Image

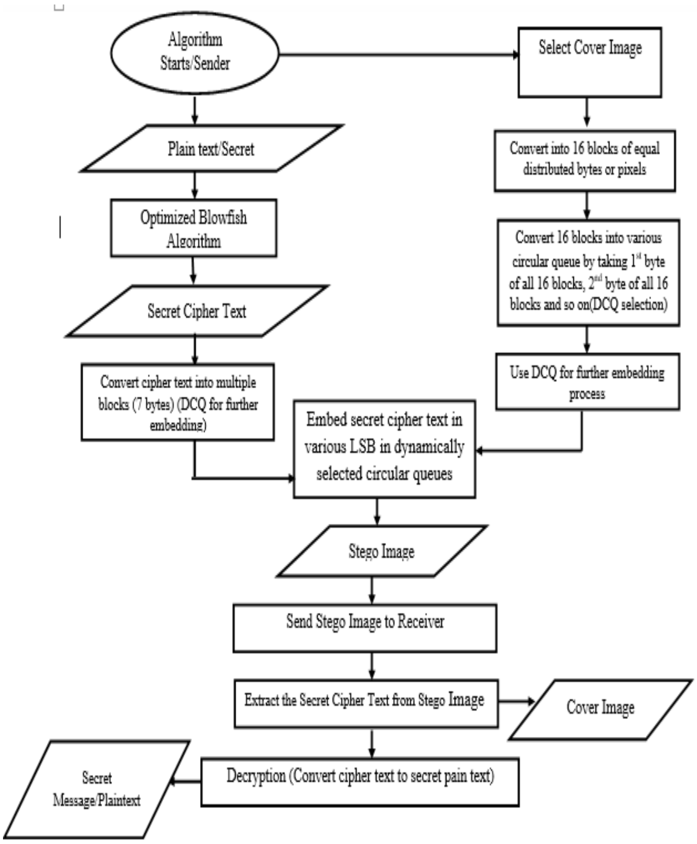
Algorithm Starts/Sender
Select Cover Image
Plain text/Secret
Convert into 16 blocks of equal distributed bytes or pixels
Optimized Blowfish Algorithm
Convert 16 blocks into various circular queue by taking 1st byte of all 16 blocks, 2nd byte of all 16 blocks and so on(DCQ selection)
Secret Cipher Text
Use DCQ for further embedding process
Convert cipher text into multiple blocks (7 bytes) (DCQ for further embedding)
Embed secret cipher text in various LSB in dynamically selected circular queues
Stego Image
Send Stego Image to Receiver
Extract the Secret Cipher Text from Stego Image
Cover Image
Secret Message/Plaintext
Decryption (Convert cipher text to secret pain text)

Figure 1. Flowchart of proposed work

4.3 Comparison Chart

This section contain the comparison between the previous work and the proposed calculated values of MSE and PSNR where it can be clearly seen that the calculated value shows some significant decrement which suggests that the proposed approach is slightly better than the previous approach. The table were generated in the MATLAB tool which was also used for the calculation of MSE and PSNR values of the output image.

Table 1. Previous and proposed MSE values

Cover Image	Previous MSE Value	Calculated MSE Value
Lena	**0.0049**	**0.0046**
Cameraman	**0.0021**	**0.0020**
Barbara	**0.0003**	**0.0002**
Baboon	**0.0004**	**0.0004**

The figure below illustrate the comparative analysis of the previous MSE value and Calculated MSE value where it can be clearly seen that the calculated value shows some significant decrement in the MSE value comparing to that of previous work.

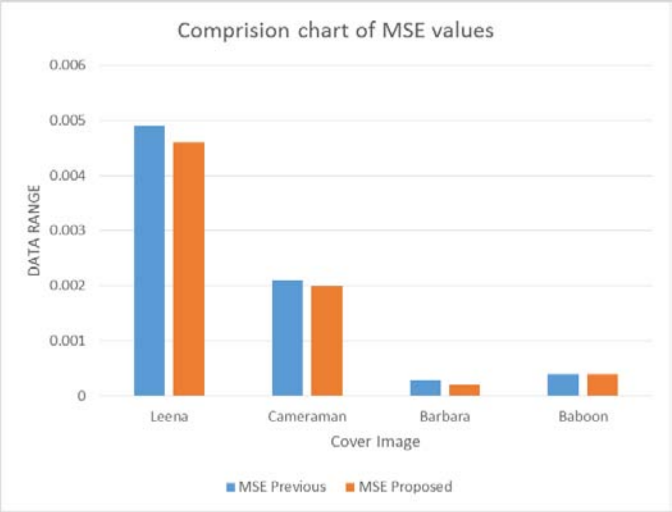

Figure 2. Comparison Chart for previous and proposed work MSE value

Table 2. Previous and proposed PSNR values

Cover Image	Previous PSNR Value	Calculated PSNR Value
Leena	**72.89**	**72.98**
Cameraman	**74.71**	**75.01**
Barbara	**82.89**	**82.94**
Baboon	**82.03**	**83.01**

The figure below illustrate the comparative analysis of the previous PSNR value and Calculated PSNR value where it can be clearly seen that the calculated value shows some significant decrement in the PSNR value comparing to that of previous work.

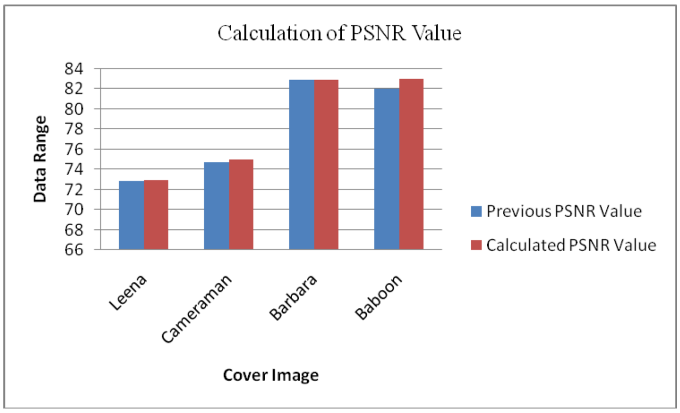

Figure 3. Comparison Chart for previous and proposed work PSNR value

V. Conclusion And Future Work

In this paper work the secret blocks of message is allocated in dynamic manner by the sending side to blocks of image in respect to the circular queues, which in turn increases the security level as well as gives the dynamic impact to the proposed algorithm. Blowfish cipher block is used in proposed algorithm to provide confidence and trust in the data centre end to end communication. At the level where we implement the steganography the LSB substitution using the circular queues are there to protect the data from getting leaked when the secret data resource is being shared among multiple transmission sites. By the analysis of the result we can say that this proposed method will increase the security of the secret data. Cloud Computing has a very vast scope and security of the data plays a major role in today’s digital world. There is much more to be improved in this area. The performance of the proposed algorithm could be enhanced using various different parameters. We hope the overhead created will affect a little, it could also be a filed to be improved in future.

VI. Acknowledgment

The satisfaction that accompanies that the successful completion of any task would be incomplete without the mention of people whose ceaseless cooperation made it possible, whose constant guidance and encouragement crown all efforts with success. I am grateful to my guide Dr. Shiva Prakash for the guidance, inspiration and constructive suggestions that helped me in the preparation of this progress report. I wish to thank my parents who have been always been a source of inspiration for their never-ending support and love throughout completion of the report and I am also thankful my friends who have helped in successful completion of the partial report.

VII. References

[1] Anderson, Ross J., and Fabien AP Petitcolas. "On the limits of steganography." IEEE Journal on selected areas in communications 16.4 (1998): 474-481.

[2] Chandramouli, Rajarathnam, and Nasir Memon. "Analysis of LSB based image steganography techniques." Image Processing, 2001. Proceedings. 2001 International Conference on. Vol. 3. IEEE, 2001.

[3] Christina L, Joe Irudayaraj V S “Optimized Blowfish Encryption Technique.” IJIRCCE Vol. 2(2014): 2320-9798.

[4] Patil, Priyadarshini, et al. "A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish." Procedia Computer Science 78 (2016): 617-624.

[5] Awwad, Yousef Bani, and Mohammad Shkoukani. "The Affect of Genetic Algorithms on Blowfish Symmetric Algorithm." IJCSNS 17.3 (2017): 65.

[6] Van Cleeff, André, WolterPieters, and Roel J. Wieringa. "Security implications of virtualization: A literature study." Computational Science and Engineering, 2009. CSE'09. International Conference on. Vol. 3. IEEE, 2009.

[7] Provos, Niels, and Peter Honeyman. "Hide and seek: An introduction to steganography." IEEE security & privacy 99.3 (2003): 32-44.

[8] Sumathi, C. P., T. Santanam, and G. Umamaheswari. "A study of various steganographic techniques used for information hiding." arXiv preprint arXiv:1401.5561 (2014).

[9] Islam, Saiful, Mangat R. Modi, and Phalguni Gupta. "Edge-based image steganography." EURASIP Journal on Information Security 2014.1 (2014): 8.

[10] Awwad, Yousef Bani, and Mohammad Shkoukani. "The Affect of Genetic Algorithms on Blowfish Symmetric Algorithm." IJCSNS 17.3 (2017): 65.

[11] Sumathi, C. P., T. Santanam, and G. Umamaheswari. "A study of various steganographic techniques used for information hiding." arXiv preprint arXiv:1401.5561 (2014).

[12] Kelvin Curran, "An Evaluation of Image Based Steganography Methods," International Journal of Digital Evidence Fall, vol. 2, Issue 2, 2003.

[13] Nag, Amitava, et al. "A novel technique for image steganography based on DWT and Huffman encoding." International Journal of Computer Science and Security,(IJCSS) 4.6 (2011): 497-610.

[14] Swain, Gandharba, and Saroj Kumar Lenka. "A novel steganography technique by mapping words with LSB array." International Journal of Signal and Imaging Systems Engineering 8.1-2 (2015): 115-122.

[15] Jain, Mamta, Saroj Kumar Lenka, and Sunil Kumar Vasistha. "Adaptive circular queue image steganography with RSA cryptosystem." Perspectives in Science 8 (2016): 417-420.