IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 8, Issue 4, April 2019

Secured Crypto-Stegano Communication

Pashang Engineer[1], Priyanka A. Bansode[2], Shreya Vitthalrao Surnar[3], Prathmesh N. Gunjgur[4]

Computer Engineering, Ramrao Adik Institute of Technology, Nerul, Navi Mumbai[1,2,3,4]

Abstract: Developing a really good efficient secure communication in an android application comes with many of the same challenges posed by the natural imbalances found in computing, Input / Output and communication bandwidths of physical systems. These challenges are greatly amplified by the huge scale of the system, its distributed nature and the fact that virtually all applications are data-intensive. To ensure the privacy and security of the data in the android applications many image processing solutions are implemented to face these challenges. This project focuses on possible image processing solutions using best-possible techniques to battle against the security threats in an android environment.

Keywords: LSB, AES, Steganography

I. INTRODUCTION

There are many transmission media to transfer the data to destination like e-mails; at the same time it is may be easier to modify and misuse the valuable information through hacking. So, in order to transfer the data securely to our destination without any changes or modifications many image processing solutions are implemented. This proposal focuses on possible image processing solutions using best possible techniques along with a stellar encryption algorithm. One of the strongest applications of image processing is steganography. Steganography deals with hiding a message, image, or file within another message, image, or file.. Generally, the hidden messages will appear to be (or be part of) something else: images, articles, shopping lists, or some other cover text. For example, the hidden message may be in invisible ink between the visible lines of a private letter. Some implementations of steganography which lack a shared secret are forms of security through obscurity, whereas key-dependent Steganographic schemes adhere to Kerckhoffs's principle.

II. LITERATURE SURVEY

Satwinder Singh and Varinder Kaur Attri discussed in their paper that at present the dual layer of security to the data, in which first layer is to encode data using Least Significant Bit image steganography method and in the second layer encrypt the data using Advance Encryption Standard Algorithm. Steganography does not replace the encryption of data, instead it does provides an extra security feature to it. In our work what we discuss is a secret text message is hiding behind the digital image file and this image file is then encrypted using the AES encryption module using the AES-256 bit length.[1]

Krati vyas and B.L.Pal discussed in their paper about security and privacy increases, need of hiding their secret information is going on. If a user wants to send their secret information to other persons with security and privacy he can send it by using image steganography. LSB changes the image resolution quite clear as well as it is easy to attack. It is clear that LSB changes the image resolution when the least significant bits add in the binary image format, so that image quality become burst and there become so much difference in the original image and encoded image in the respect of image quality. So to overcome this problem, In this thesis we suggested modifying the LSB technique so that we can get same image quality as it has before the encoding.[2]

In recent years, the rapid growth of information technology and digital communication has become very important to secure information transmission between the sender and receiver. e.g., image, audio and video files. In this paper, a new algorithm for image steganography has been proposed to hide a large amount of secret data presented by secret color image. This algorithm is based on Different Size Image Segmentations (DSIS) and Modified Least Significant Bits (MLSB), where the DSIS algorithm has been applied to embed a secret image randomly instead of sequentially; . The simulation results justify that the proposed approach is employed efficiently and satisfied high imperceptible with high payload capacity[4].

In another paper by Hamdan Lateef Jaheel and Zou Beiji we combined two steganography algorithms namely J. Steg and Out Guess algorithms, in order to exploit the beneficial characteristics and features of both algorithms to enhance the protection level for secret images. In their proposed approach, the secret message (image) is first concealed inside another image using J Steg algorithm and the resultant stego-image is further hidden inside a final image using Out

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 8, Issue 4, April 2019

Guess 0.1 algorithm. In this combine approach, the tricky nature of hiding an already hidden message is using two different algorithms increases the level of difficulty for a third party to suspect the existence of a secret image in the first place or even successful decode the it. Besides that, the priority given to the choice of a good image size and type in this approach further disguises the secret image and increases the chances that the image could go unnoticed. Results after calculating the capacity and PSNR for images proved that the approach is a good and acceptable steganography system. The model presented here is based on JPEG images.[5]

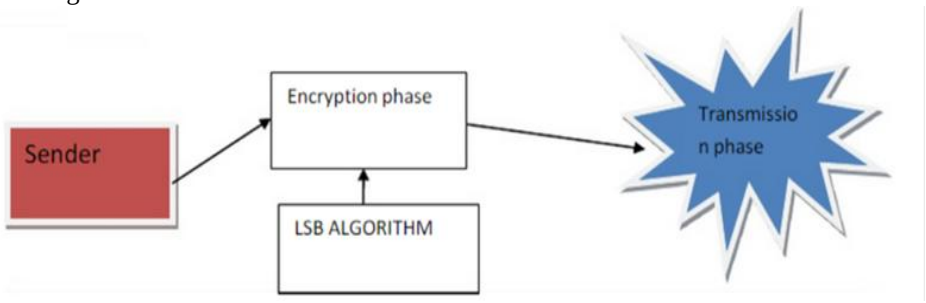
The main advantage of this system is a mixed combination of cryptography and steganography which provides a double layer security which we don't see in many existing android applications in the play store

III. PROPOSED SYSTEM

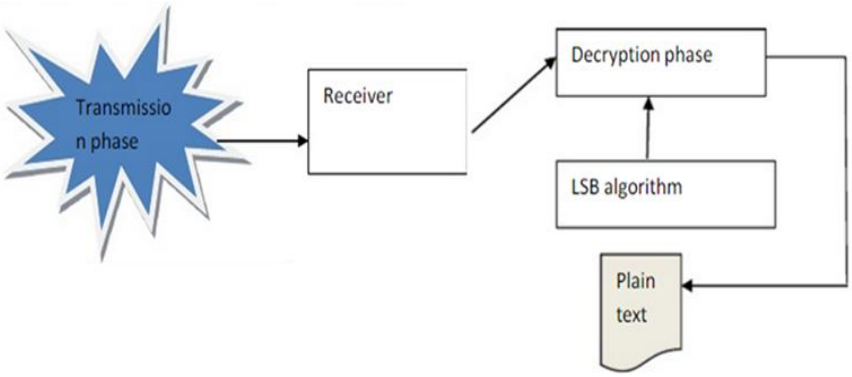
What we are proposing an effective and reliably flexible system with explicit dynamic data support to ensure the proper usage of data . A unique secret key is shared between two people namely sender and receiver ensuring data security even more.Tight security and performance analysis shows that the proposed scheme is highly efficient against dangerous data modification attacks, and even server colluding attacks. In our system, there is combination of cryptography and steganography which makes my system much more useful.

The Proposed system will consist of three types of modules:

- **Encryption module:** The "Encryption phase" uses two types of files for encryption purpose. The first is a secret file which is to sent securely to the receiver, and the other is a carrier file much like an image file. In this encryption phase, the data is embedded into the image using "Least Significant Bit algorithm" (LSB) by which the least significant bits of the secret document(our source data) are arranged with the bits of carrier file such as image, Such that the message bits will merge with the bits of carrier file. In this procedure LSB algorithm helps for securing the originality of image.After that in order to provide strong security we use AES-256 bit encryption to ensure data security providing a double threat to our algorithm.



- **Decryption module:** The Decryption phase is the bang opposite to the below encryption phase we just discussed now. In decryption phase, the image file i.e. in which the source data is hidden is given as an input file to be sent. The decryption phase uses that same shared password which was given for the encryption and given to the receiver to open the image file. After correct password is given, the decryption section uses the LSB algorithm by which the encoded bits in the image is deciphered and then instead of the original image we see the data but in encrypted format. It's over here that we use AES algorithm.

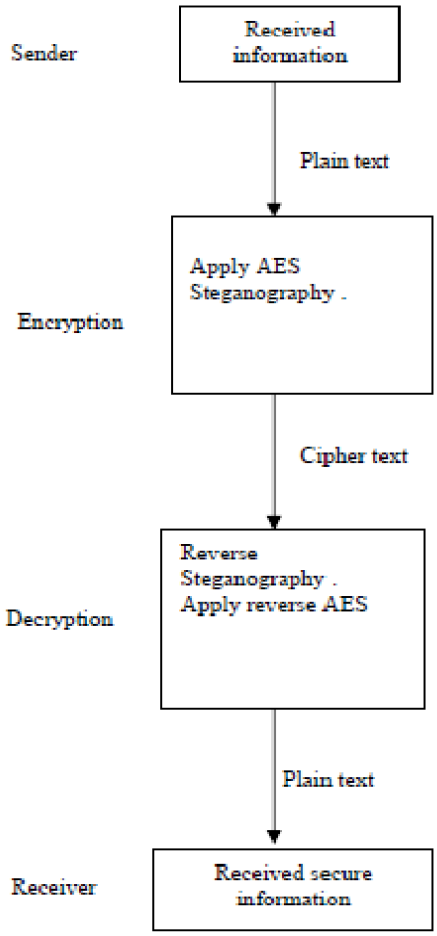


IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 8, Issue 4, April 2019



A. Advantages of proposed system

- The main advantage of this system is a mixed combination of cryptography and steganography which provides a double layer security and more efficient means to transfer data.
- It provides a Higher PSNR (Peak signal-to-noise ratio) to other algorithms mentioned above
- There is no image degradation or blurriness.
- It is also less time consuming comparatively to other existing systems that we discussed.
- The fact that we combine two very known and strong algorithms also ensures security to our systems. These algorithms have been known to be invulnerable to attacks.

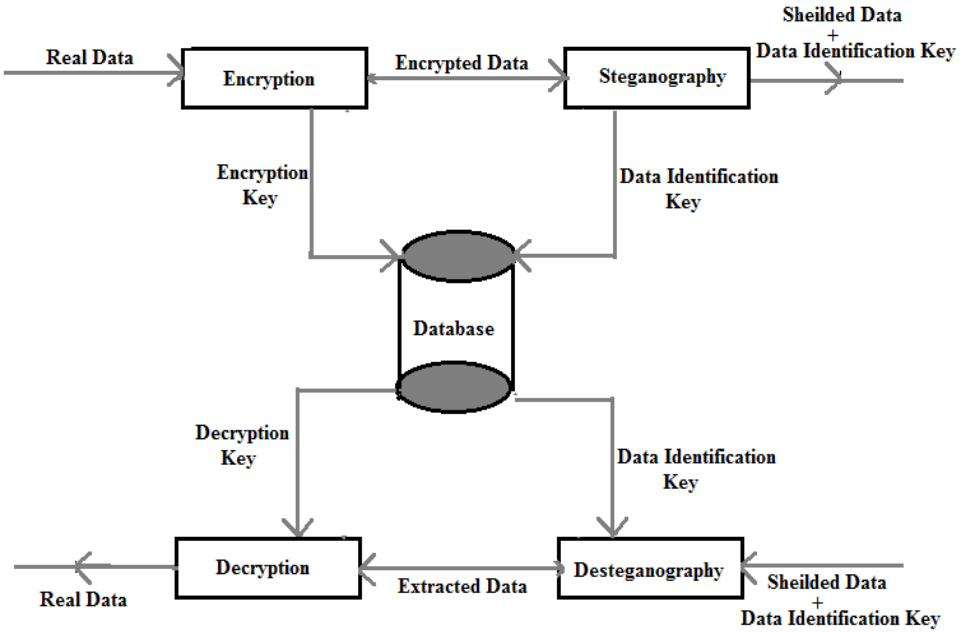
B. System design

The system design consisting of the encryption, decryption, database ,steganography, de-staganography along with encryption key and the data encryption key are the modules with which this system operates. The procedure is simple actually i.e .real data goes through the encryption software namely our AES algorithm using the latest 256 bit along with an encryption key which will also be used for decryption. This then goes through steganography providing a double protection against majority of data attackers. The image saved is then shared or sent to the receiver after which it decrypts the image using the shared key mentioned above.

Architecture consists of four basic blocks

1) Encryption: Matrix Mapping Method For Symmetric Key Cryptography.
2) Steganography: Least Significant Bit
3) Decryption: Matrix Mapping Method for Symmetric Key Cryptography.
4) Desteganography: Least Significant Bit Extraction.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 8, Issue 4, April 2019



C. Lsb module

1.Least Significant Bit Embedding

- LSB (Least Significant Bit) substitution is the process of adjusting the least significant bit pixels of the carrier image. It is simple approach embedding message into the image.
- Let's say for an 8 -bit image, the least significant bit i.e. the 8th bit of each byte of the image is changed to the bit of secret message.
- LSB is effective in using BMP images since the compression in BMP is almost lossless.
- The embedding technique we use in this algorithm is based on replacing the LSB of the pixel (I(i,j)) with the message bits one by one. Hence if the message is equivalent to m-bits there are m-pixels to deal with, whose least significant bits will be replaced by the m-message bits. The embedding procedure can be described using the equation as follows:
- In general, a p-by-q image is simply a p-by-q matrix, where each entry in the matrix is a positive integer called the pixel value, which determine the color of that pixel. For an n-bit
- image, these pixel values range from 0 to 2n " 1. In other words, the possible color values for each pixel in an n-bit image are the colors corresponding to the bit strings of
- length n. Unless there is a specific need to use the bit string representations of pixel values, we will typically use the decimal representations. In this paper, we talk primarily
- about 8-bit grayscale images. These images are thus p-by-q matrices of integers which range from 0 to 255, where 0 corresponds to black, 255 to white, and the values in between form a spectrum of varying shades of grey (i.e., darker shades nearer 0 and lighter shades nearer 255). The least significant bit (LSB) is the bit corresponding to 20, that is, the bit that makes a value even or odd. Since these grayscale values range from in order dark to light, each grey value varies little from the values on either side of it. For example, the grey value 100 varies little from the grey values 99 or 101. Therefore, changing the LSB creates an imperceptible change in the image.

Steganography

Step 1: Convert pixels into Binary format

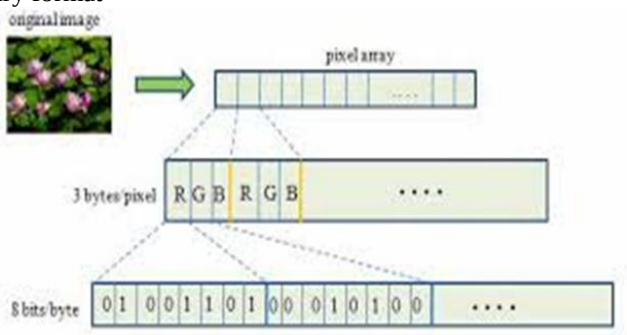


Figure Convert pixels into Binary format

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 8, Issue 4, April 2019

Step 2: Convert text data into binary format

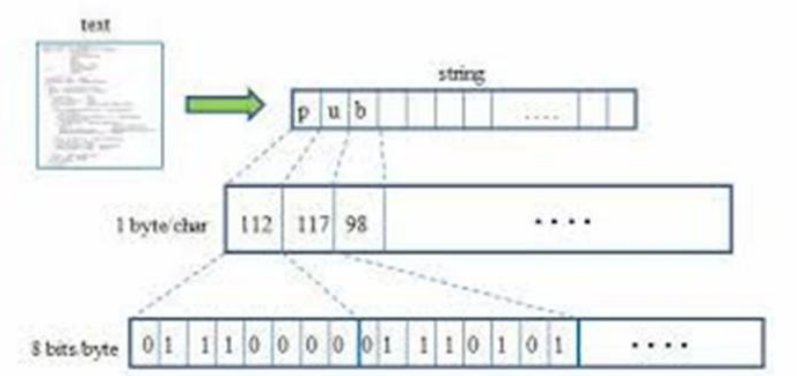


Figure: Convert text data into binary format

Step 3:Insert text bits into image bytes

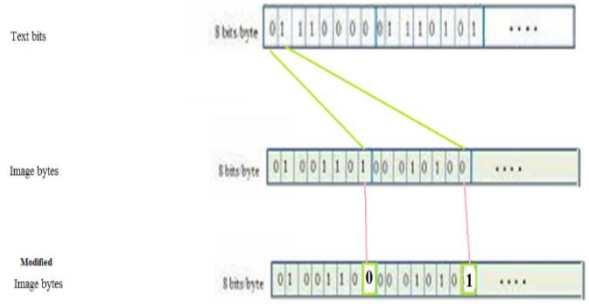


Figure :Convert text data into binary format

Step 4:Reverse-Steganography

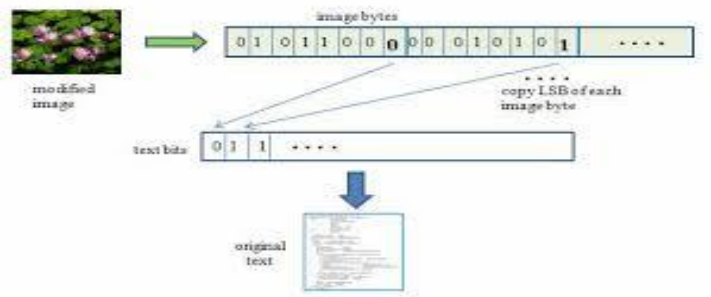


Figure 4.1.4: Reverse- Steganography

D. Algorithm:

Step 1: Read the cover image and text message which is to be hidden in the cover image.
Step 2: Convert text message in binary.
Step 3: Calculate LSB of each pixels of cover image.
Step 4: Replace LSB of cover image with each bit of secret message one by one.
Step 5: Write stego image
Step 6: Calculate the Payload Capacity, Mean square Error (MSE), Peak signal to noise ratio (PSNR) of the stego image.

E. AES Algorithm:

The definition Advanced Encryption Standard or AES states that AES is a symmetric block cipher used by the U.S. government to protect classified information and is implemented in software and hardware throughout the world to encrypt sensitive data.The AES algorithm used in our system is simply made to further protect our data. Steganography will simply do it's thing by implementing it's LSB algorithm. After applying LSB, we will be applying AES algorithm to further ecrypyt the data in case the user or let's the use the term "hacker" gets access to our system by hacking into the LSB algorithm he will have to face the encrypted data which is encrypted using AES-256 bit.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 8, Issue 4, April 2019

Traditionally, AES comprises of three block ciphers, AES-128 bit, AES-192 bit and AES-256 bit. Now each cipherencrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128-bits, 192-bits and 256-bits, respectively. Symmetric or secret-key ciphers use the same key for encrypting and decrypting, so both the sender(being the client) and the receiver(let's say me) must know and use the same shared secret key. There are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys -these rounds consists of several processing steps and go through methods like substitution, transposition and mixing of the input plaintext format and transform it into the final required output of ciphertext format.

The AES-256 bits module will particularly provide us a better security with my LSB technique and the AES module for encryption of the text.

AES-256 bit

The AES-256 bit algorithm was actually first used by the US governments to probably fight against cybercrime. Because of the length of the key (i.e.256 bits) and the number of hashes (14), it takes a really long time for a hacker to perform an attack. Therefore the added benefit right there is an attack like a dictionary attack performed by an hacker wouldn't work considering the amount of time it would take to decrypt the underlining text.

F .Steps for Algorithm:

1. Key Expansions—The round keys are which derived from the cipher key using Rijndael's key schedule. Now ,AES algorithm requires a separate 128-bit round key block for each round plus one more.

2. Initial Round

1. Add Round Key—each byte of the state is combined with a block of the round key using bitwise xor.

3. Rounds

1. Sub Bytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.
2. Shift Rows—a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.
3. Mix Columns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.
4. Add Round Key

4. Final Round (no MixColumns)

1. Sub Bytes
2. Shift Rows
3. Add Round Key.

IV. PERFORMANCE ANALYSIS

1.Cover image: It is defined as original image into which required information is embedded .it is also called carrier image.

2.Stego image: It is an unified image obtained by combination of cover and payload image.

B: Error Analysis :

1 .The Mean Square Error (MSE): Mean square error and the Peak Signal to Noise Ratio (PSNR) are the two error metrics used to compare image compression quality. The MSE represents the cumulative squared error between the compressed and the original image, whereas PSNR represents a measure of the peak error. The lower the value of MSE, the lower the error.

$$MSE = \frac{1}{m\,n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

2. PSNR: To compute the PSNR, the block first calculates the mean-squared error using the following equation: In the previous equation, M and N are the number of rows and columns in the input images, respectively. Then the block computes the PSNR using the following equation:

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

Table1.Lsb Embedding Based Results for image Steganography

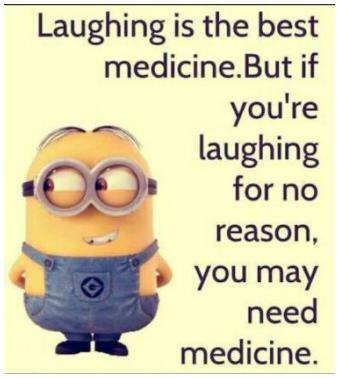
IMAGE	MSE	PSNR
MINIONS	0.0595	60.38
BABY	0.0885	55.65

IJARCCE

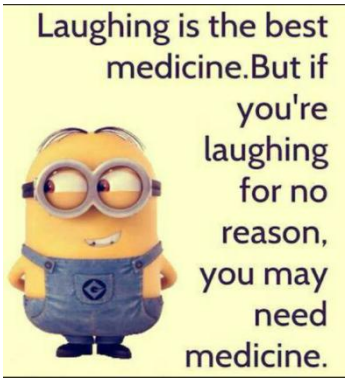
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 8, Issue 4, April 2019



Original Image (MINIONS)



Steganographic Image(MINIONS)

Table 2. MSE and PSNR values for the Original and Stego images

Cover image	Stego Image	Amount of data embedded	MSE %	PSNR (dB)	Amount of data extracted
MINIONS (29.6 kb)	Stego-MINION (212 kb)	4267 bytes	0.48	51.28	4267 bytes
BABY (47.18 kb)	Stego- BABY (467 kb)	4513 bytes	0.41	51.93	4513 bytes

Original Image (BABY)

Steganographic Image (BABY)

V. CONCLUSION AND FUTURE ENHANCEMENT

This android application overcomes the disadvantages of existing systems in the play store especially as it provides better security and lesser of an image being of bad quality or as they say “blurry” . Steganography especially combined with an encryption algorithm like aes-256 bit, is a powerful tool which enables people to communicate without possible hackers targeting your system. The above proposed method provides good image quality with very little distortion in the image. The main advantage of this system is a mixed combination of cryptography and steganography which provides a double layer security which we don’t see in many existing android applications in the play store.

REFERENCES

[1]. Satwinder Singh, Varinder Kaur Attri : ” Dual Layer Security of data using LSB Image Steganography Method and AES Encryption Algorithm”, International Journal Of Signal Processing, Image Processing And Pattern Recognization,Vol.8,No.5(2015), pp.259-266

[2]. Krati vyas, B.L .Pal : ”A Proposed method in Image Steganography to Improve Image quality with Lsb Technique” International Journal Of Advanced Research In Computer And Communicational Engineering.Vol.3,1 january 2014

[3]. Sandeep Kumar:”Image Steganography using Improved Lsb and Exor Encryption Algorithm” School of Mathematics and Computer Applications Thapar University Patiala– 147004 JULY 2014.

[4]. Odai M. Al-Shatanawi, Nameer N. El. Emam: “A New Image Steganography Algorithm based on mlsb method with Random Pixels Selection” International Journal of Network Security & Its Applications (IJNSA) Vol.7, No.2, March 2015

[5]. Hamdan Lateef Jaheel , Zou Beiji:” A Novel approach of combining Steganography Algorithms” international journal on smart sensing and intelligent systems vol. 8, no. 1, march 2015

[6]. Balakrishana, C., Chandra, V. N. & Pal, R., “Image Steganography Using Single Digit Sum with Varying Base”, International Conference on Electronics, Computing and Communication Techonologies (CONECCT), pp.1-5, 2014.