# A Combined Approach of Steganography and Cryptography Technique based on Parity Checker and Huffman Encoding

Abdelmged A. A.
Computer Science Department
Minia university, Egypt

Al-Hussien Seddik Saad
Computer Science Department
Minia university, Egypt

Nada Hussien
Computer Science Department
Minia university, Egypt

## ABSTRACT
Steganography and Cryptography are two popular ways of sending vital and pivotal information in a secret way. But neither cryptography nor steganography alone can guarantee better security because they can be cracked after some efforts. So it is necessary to combine both cryptography and steganography to generate a hybrid system called as Crypto-Steganography. Cryptography is the art of saving information by encrypting it into an immersed format. On the other hand, steganography is the art and science of secret communication to send messages in a way which hides even the existence of the communication. This paper aims to improve a new approach of hiding a secret message in an image, by taking advantages of combining cryptography and steganography. Which using the Huffman coding to compress the message and RC4 algorithm to encrypt the secret message then the cipher text embedded in the cover image using Parity checker algorithm using blue layer only. The results showed that the proposed method gives better results of higher PSNR lower MSE.

## Keywords
Cryptography, Steganography, Cipher text, Huffman Coding, Parity checker.

## 1. INTRODUCTION
Because internet is one of the most important factors of information sharing and communication; and increasing in the number of attacks recorded during exchange of information between the source and intended destination as well as unauthorized usage of stored secret information has indeed called for a more robust method for securing data transfer and storage. Cryptography and steganography are the two popular methods available to provide security. One hides the existence of the message and the other distorts the message itself [1]. which the Cryptography is the art of achieving security by encoding the data into unreadable form. Data that can be read and understood without any difficulty is called plain text or clear text. The method of encoding Plain text in such a way as to hide its content is called encryption. Encrypting plain text results in unreadable gibberish called cipher text. By combining both the techniques, more robust security can be achieved. The major difference between the two is that cryptography protects the content of a message and steganography hide the message.

### 1.1 Cryptography
The term cryptography came from Greek word kryptós means hidden, secret"; and graphein, means "writing"[2]. It is techniques for scrambling a message so it cannot be understood. In cryptography the original text (plain text) is encrypted and converted into cipher text. The method used to recover original text from the cipher text is Cryptanalysis or decryption.

### 1.2 Types of Cryptographic Algorithms
The type of cryptography can be divided into [3]:

Symmetric key: Also known as single or secret key cryptography uses a single key both for encrypting and decrypting the plaintext. This type is used in this paper according to Figure (1).

Asymmetric key: Too known as public key cryptography uses different keys for encrypting and decrypting the information.

Hash values: Uses a mathematical transformation to irreversibly "encrypt" information.

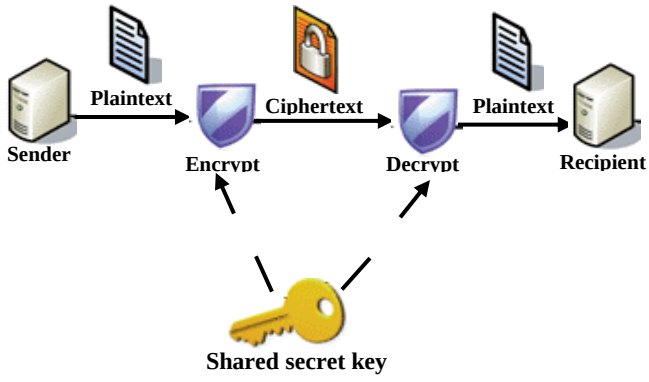



**Fig.1 Cryptography model with symmetric key**

### 1.3 Cryptography Serves Following Purposes [4]
1. **Confidentiality:** The principle of confidentiality assigns that only the sender and the intended recipient should be able to arrival the contents of a message.
2. **Authentication:** Authentication mechanisms help to ensures and confirms a user's identity. This process ensures that the origin of the message is correctly identified.
3. **Integrity:** The integrity mechanism ensures that the contents of the message remain the same when it reaches the intended recipient as sent by the sender.
4. **Non- repudiation:** Non-repudiation does not allow the sender of a message to refute the claim of not sending the message.

## 1.4 Steganography

The term steganography came from Greek words "Steganos" & "graphein" which together means "Concealed writing" [2]. Steganography is a science of masking a secret data within another message, image, audio, video or protocol, etc., which results is stego_media.

The main terminologies used in the steganography are the cover file (carrier), payload (secret message), stego file, hiding capacity and stego key according to this Figure (2) [5]

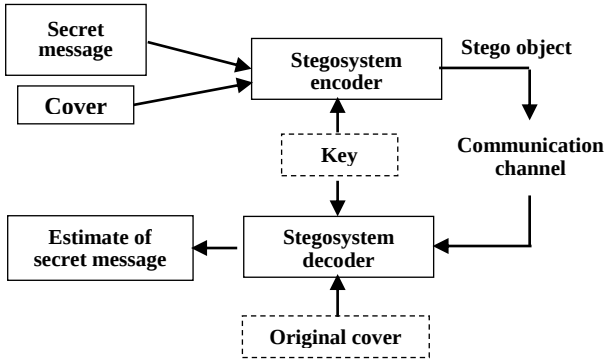



**Fig.2 Basic steganography system**

a) **Cover file (Carrier):** It is defined as the original file into which the required secret message will be embedded. It is also termed as innocent file or host file. The secret message should be embedded in such a manner that there are no significant changes in the properties of the cover file.

b) **Payload (Secret Message):** It is the massage that has to be embedded within the cover file in a given steganography model. The payload can be in the form of text, audio, images, or video.

c) **Stego file (stego-object):** It is the final file obtained after embedding the payload into a given cover file.

## 1.5 Steganography Approaches

The steganography approaches can be divided into three types. [6]

1. **Pure Steganography:** This technique simply uses the steganography approach only without combining other methods. It is working on hiding information within cover carrier.
2. **Secret Key steganography:** The secret key steganography uses the combination of the secret key cryptography technique and the steganography approach. The idea of this type is to encrypt the secret message or data by secret key approach and to hide the encrypted data within cover carrier.
3. **Public Key Steganography:** The last type of steganography is to combine the public key cryptography approach and the steganography approach. The idea of this type is to encrypt the secret data using the public key approach and then hide the encrypted data within cover carrier.

## 1.6 Type of Compression

There are two types of compression, Lossless and Lossy compression, in lossless data compression original data is exactly restored after decompression. Mainly used for text data compression and decompression. It can also be applied to image compression. The popular algorithms are the run length coding, Huffman coding, adaptive Huffman coding, arithmetic coding and dictionary based coding. In lossy data compression original data is not exactly restored after decompression and accuracy of re-construction is traded with efficiency of compression. Mainly used for image data compression and decompression. Lossy data compression algorithms are transform coding (for example, discrete cosine transform), and wavelet based coding (for example, continuous wavelet transform-CWT and Discrete wavelet transform (DWT).

## 1.7 Huffman Code

It is one of the lossless data compressions; it was developed by David A. Huffman while he was a Ph.D. student at MIT, and published in the 1952 paper "A Method for the Construction of Minimum-Redundancy Codes". Huffman code is an algorithm to compression based on the frequency of occurrence of a symbol in the file that is being compressed. The easiest way to see how this algorithm works the can show the example to compression the message (ABEACADABEA). A Huffman tree is constructed which is the button-up approach according of the following steps:

- Remember the frequency of each character within the message as a list as proven within the Table 1.
- Sort the list by frequency and make the two lowest elements into leaves, creating a parent node with a frequency that is the sum of the two lower element's frequencies [8].
- The two elements are removed from the list and the new parent node is inserted into the list by frequency. So now the list, sorted by frequency [8].
- You then repeat the loop, combining the two lowest elements.
- You repeat until there is only one element left in the list.

**Table 1: the frequencies and probabilities of the text 2 (ABEACADABEA)**

| Symbol | Frequency | Probability |
|---|---|---|
| **A** | 5 | 5 / 11 = 0.45 |
| **B** | 2 | 2 / 11 = 0.18 |
| **C** | 1 | 1 / 11 = 0.09 |
| **D** | 1 | 1 / 11 = 0.09 |
| **E** | 2 | 2 / 11 = 0.18 |

To generate a Huffman code, you traverse the tree to the value you want, outputting a 0 every time you take a left hand branch and a 1 every time you take a right hand branch [8]. Figure 3 illustrate the Huffman tree for the text (ABEACADABEA).

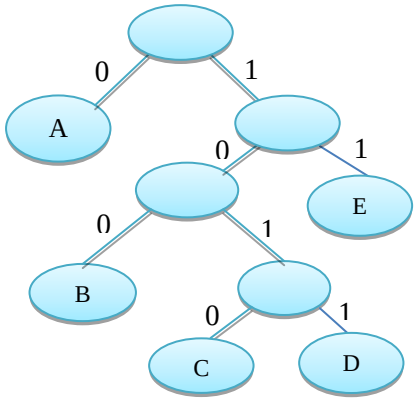



**Fig. 3 Huffman tree to (ABEACADABEA)**

According the above Huffman tree, the obtained code word is described in table 2.

**Table 2: The code word of the text (ABEACADABEA) using Huffman tree**

| Symbol | Code word |
|---|---|
| **A** | 0 |
| **B** | 100 |
| **C** | 1010 |
| **D** | 1011 |
| **E** | 11 |

After Huffman tree is finished to the text (ABEACADABEA) the code word is obtained (23 bit): 01001101010010110100110. While the message in ASCII code is represented as 88 bits (11 characters × 8 bits), so Huffman code saves more than 25% in the size of the message.

The rest of this paper is organized as follows. In section 2, some related methods that have been presented to improve image steganography and cryptography techniques will be briefly explained. In section 3, the proposed method will be discussed in details. Section 4 contains experimental results and discussion of the proposed method and finally section 5 concludes the paper.

## 2. PREVIOUS WORK

In paper [9], a new way of hiding information in an image with less variation in image bits have been proposed, which makes technique secure and more efficient than LSB, according to this technique a steganography and cryptography methods has been used together. Which it's used advanced LSB (Least Significant Bit) and also applied a cryptographic method RSA algorithm to secure the secret message so that it is not easy to break the encryption without the key. RSA algorithm itself is very secure that's why they used in this technique to increase the security of the secret message.

In paper [10], the author has been proposed a method which all pixels of the cover image can be used but message bit is stored in LSB of one of the three color components, Red(R), Green (G), Blue (B) in alternate fashion based on the parity of three LSBs of R, G, and B components of 24-bit color image. The proposed work uses the concept of parity method for hiding and recovering secret data or information. The proposed method has been hidden large volume of data in a single RGB image with changes in only few pixels of input image retaining the advantages and discarding the disadvantages of traditional LSB method.

In [11], this paper has been proposed approach provided a double layer protection and can hide a large amount of information because all three channels of an image have been used for data hiding. Which the secret message has been encrypted using RSA algorithm and hidden into random pixels of the cover image in different planes. Hiding data into random pixels is more efficient than the sequential embedding. The attacker cannot get clues that secret message has been hidden in the cover image. If the attacker knows about the existence of secret message, cannot decrypt it without the proper key. And also explained a method that extracted the encrypted information at the receiving end and decryption of it to get original messages and helps to achieve better capacity and immunity to suspicion.

In [12], the author has been proposed a new steganography method the method has been represented the character by six binary bits by using LSBraille method (Braille method of reading and writing for blind people) instead of using the ASCII encoding format. In this method, three bits of the message are hidden in a single pixel, and a true image is composed of three layers (Red, Green, and Blue) layer. Two bits are embedded in the Blue layer, and one bit is embedded in the green layer of the same pixel. In the Blue layer, the message is not only embedded in the least significant bit (LSB), but also the second and the third LSB may be changed. However, during each process of embedding, only one bit of the Blue layer is changed. This process has been done by taking the last three bits of the Blue layer pixel and entered it in the XOR Gate, and applying some equations. From the experimental results, it is found that the proposed method achieves a very high Maximum Hiding Capacity and Peak Signal-to- Noise Ratio.

In paper [13], A combination of steganography and cryptography has been used which take advantage of both the techniques. This method has been used Blowfish Encryption Algorithm for encrypting the message to be hidden inside the image for making it non readable and secure. After encryption they applied LSB technique of steganography for further enhancing the security. So that combination of steganography and cryptography for improving the security.

In paper [14], a new image steganography method has been proposed. The proposed method hides the secret message inside the cover image by representing the secret message characters using Braille method of reading and writing for blind people. Which all pixels of the cover image can be used and message bit has been stored in LSB of one of the three color components Blue (B) only; based on the parity of three LSBs of R, G, and B components of 24-bit color image. If the parity is even and wanted to embedded (1) Reverse LSB of blue layer and if wanted to embedded (0) no change occurred. And if the parity is odd and wanted to embed (0) Reverse LSB of blue layer and if wanted to embedded (1) no change occurred.

In [15], this paper has been proposed an encrypting system which combines techniques of cryptography and steganography with data hiding. Instead of using a single level of data encryption, the message has been encrypted twice. Then the cipher is hidden inside the image in encrypted format for further use. It uses a reference matrix for selection of passwords depending on the properties of the image. The image with the hidden data is used for further purposes.

In [16], this paper has been proposed a new image steganography technique in embedding phase the image transformed from time domain to frequency domain using discrete wavelet decomposition technique (Haar). The text message encrypted twice first: using RC4 algorithm and second using Rijndeal algorithm. Finally; the Least Significant bit (LSB) algorithm used to hide secret message in high frequency.

In [17], this paper has been presented a novel algorithm for image steganography based on effective channel selection technique is used in order to hide secret data in cover-image. Proposed work is concentrated on 8 bits of a pixel (8 bits of blue component of a randomly selected pixel in a 24-bit image), resulting better quality of image. Proposed technique has also used contrast sensitivity function (CSF) and just noticeable difference (JND) Model.

# 3. PROPOSED TECHNIQUE

Cryptography alone, or steganography alone can't make the data secure efficiently so a better technique is developed by combining these two techniques. A combination of steganography and cryptography is used which will take advantage of both the techniques [13]. So that information to be hide is first compressed using Huffman coding then encrypted using cryptography algorithm to convert information in cipher information, then this cipher information is hidden inside cover using steganography algorithm. As shown in Figure 4.

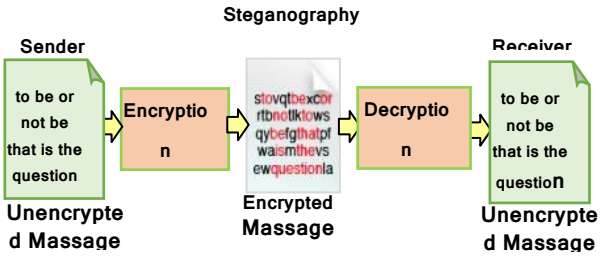



**Fig.4 Model of steganographic method with cryptography**

The steps of the steganography with cryptography system as following:

**1. Select Image**

In this step select image as a cover mage. Which has been used it to hide the secret message after encoding it in the cover image. That image may be in 24 bit images or 8 bit images**.** But in this paper deal with 24 bit images**.**

**2. Compressed The Message Using Huffman Codding.**

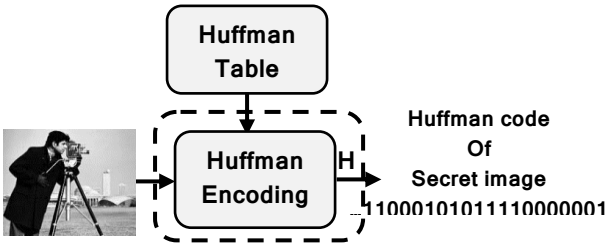



**Fig. 5 Huffman encoding of secret message (or image)**

The second step Perform Huffman encoding on the secret message to compress the message (or image) so that the capacity of the message has been increased.as shown in Figure (5).

**3. Encryption with RC4**

Before embedding the secret information in the cover image; encrypted it using RC4 algorithm and converted it into cipher text. The RC4 Encryption Algorithm, developed by Ronald Rivest of RSA, is a shared key stream cipher algorithm requiring a secure exchange of a shared key. The symmetric key algorithm has been used identically for encryption and decryption such that the data stream is simply XORed with the generated key sequence. At the time of encryption, data is send along with the public key.

**4. Embedding Process Using Parity Checker Algorithm**

In this step, the parity checker algorithm is used [14], to embed the secret message in the cover image after encrypted it (cipher text). Which the concept of even and odd parity by using the parity checker has been used by Rajkumar et al [18]. As it is already known that even parity means that the pixel value contains even number of 1's and odd parity means that the pixel value contains odd number of 1's. And determine that by collecting the three LSBs bits of the (Blue layer only) in each pixel. Now the sequence of these three bits may have either even number of 1's or odd number of 1's. If it's even parity that's mean the pixel value contains even number of 1's) and odd parity means that the pixel value contains odd number of 1's. After identifying the parity, the embedding in the proposed algorithm depends on the message bit and the parity generated by the three LSB bits of the Blue layer the embedding algorithm is as follows:

**Input:** Cover Image, Secret message
**Output**: Stego Image

**Algorithm in steps:**

1. Get the message to be embedded
2. Compressed the message using Huffman coding.
3. Encrypt the message into cipher text by using RC4 algorithm.
4. Calculate the size of the message (no. of character or byte)
5. Let N=length of cipher text in bits.
6. Select a cover image.
7. Then make loop from I=1: N.
8. Represent the cover image into three layers (R-G-B).
9. Convert the (Blue) layer to binary number (8-bits) and take the three LSBs of each pixel of the blue layer and make group of them.
10. Determine the parity of three LSBs of the blue layer (Even or Odd)
11. Get message bit (0 or 1)
12. If message bit is 0 and parity is even, do nothing
13. If message bit is 0 and parity is odd, reverse the value of the LSB of the blue layer.
14. If message bit is 1 and parity is even, reverse the value of the (BLSB)
15. If message bit is 1 and parity is odd, do nothing
16. I= I+1
17. Then collect the three layers and return the image which it's called stego image after embedding the message.
18. END.

# 4. EXPERIMENTAL RESULTS

In this section, the proposed method has been tested using their images according to Table 3.

**Table 3: Cover Images**

| Baboon | Boat |
|---|---|
|  |  |
| **Flinstone** | **Bird** |
|  |  |
| **Lena** | **Pepper** |
|  |  |

This used two algorithms (cryptography and steganography) by taking different messages with different lengths and hiding them in some cover images and comparing it with different method. The results that are obtained from these experiments are recorded and can be summarized in Table 4, Table 5 and Table 6.

**Table 4: Comparison between (LSB-3), (ZOH) Methods and Proposed method**

| Cover images | Message Capacity | PSNR | | |
|---|---|---|---|---|
| | | LSB – 3 | ZOH | Proposed method |
| Boat | 8,160 | 39.1132 | 49.9386 | 58.9207 |
| Bird | 8,160 | 39.0955 | 49.9167 | 58.9263 |
| Flinstone | 8,160 | 39.1188 | 49.9513 | 58.9309 |

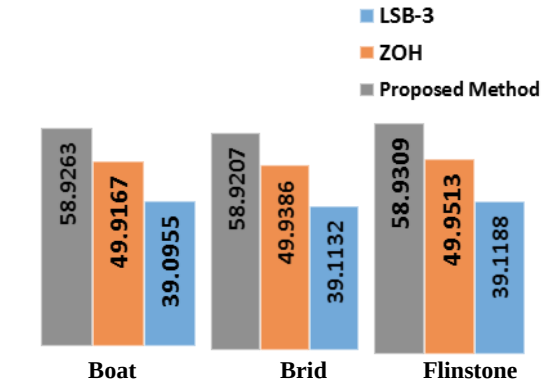



**Fig. 7 Comparison between PSNR values in Table 4**

According to the comparative results in Table 3, and Figure5, it is found that the PSNR of our method is better than that the LSB-3, and ZOH methods [19]. In addition, the stego image quality of our method is very high relative to the LSB-3, and ZOH methods.

**Table 5: Comparison between (Method [12]) and (Proposed method)**

| Cover images | Message Capacity (bytes) | PSNR | |
|---|---|---|---|
| | | Method [12] | Proposed method |
| Lena | 1000 | 63.0432 | 67.0127 |
| Baboon | 1000 | 63.0220 | 67.9955 |
| Pepper | 1000 | 63.0535 | 67.0680 |

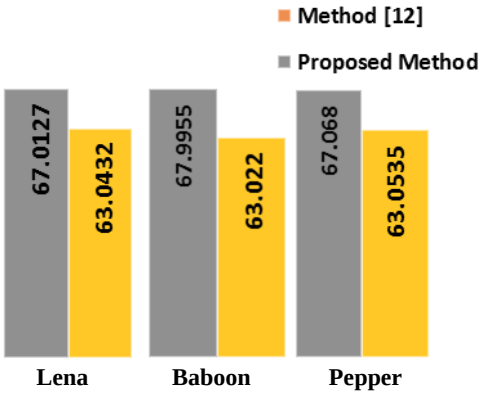



**Fig.8 Comparison between PSNR values of Table 5**

Table 5, and Figure 8 also represent the comparative results of proposed method and method [12] by using (1000) byte (secret message character) and 256 x 256 cover image (Lena, Baboon, and Pepper).and it is found that the PSNR of our method is better than that the other method.

**Table 6 Comparison between (MSLDIP), (MSLDIP-MPK) Methods and Proposed method**

| Cover images | Message Capacity (bytes) | PSNR | | |
|---|---|---|---|---|
| | | MSLDIP | MSLDIP-MPK | Proposed method |
| Lena | 6,656 | 48.6800 | 50.58189 | 58.8268 |
| Baboo | 6,656 | 48.6802 | 50.15226 | 58.8079 |
| Boat | 6,656 | 48.3541 | 50.24284 | 58.7838 |

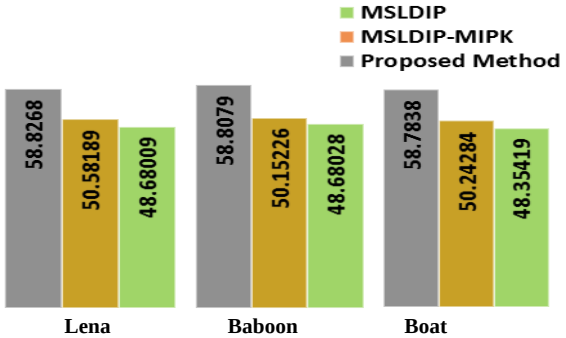
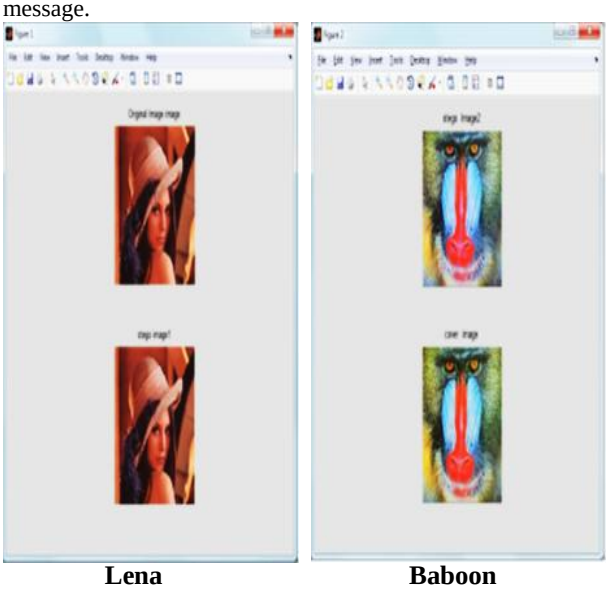



**Fig. 9 Comparison between PSNR of Table 6**

Finally in Table 6, and Figure 9 after hiding the same message length 6,656 bytes in the cover images (Lena, Baboon, Boat) with size (256 x 256), using the (MSLDIP) , (MSLDIP –

MPK) methods [20] and proposed method, it has been found that, the proposed method has higher PSNR values than the (MSLDIP) and(MSLDIP-MPK). In the last, Figure 10 shows the cover image and stego image after embedding the secret message.



**Lena** **Baboon**

**Fig.10 Cover image and Stego-image of the Lena and Baboon images**

## 5. CONCLUSIONS

In this paper, a new approach has been presented for the combination of cryptography and Steganography using Huffman coding to compress the message and RC4 algorithm for encrypting the secret message so it is become very secure and used Parity checker algorithm to hide the cipher text in to the cover image which it is very hard to detect because the proposed approach provides double layer protection, a comparative study has been done and the experimental results founded that the proposed method is considered an effective method which achieved high level of capacity, higher PSNR for security and lower MSE for robustness against attacks. As a future work, A new image steganography method will be developed so frequency domain like DWT algorithm will be used instead of special domain and develop the cryptography method by using asymmetric method like RSA method to enhance the security.

## 6. REFERENCES

[1] Tasnim M. S., Dipesh. G. K.,"Data Security Enhancement with Crystography – A Combination of Cryptography and Steganography", International Journal of Darshan Institute on Engineering Research and Emerging Technology Vol. 4, No. 1, pp. 01-06, 2015.

[2] Dipalee B.," New robust LSB steganographic technique for increased security", International Journal of Engineering Research and General Science Volume 3, Issue 2, March-April, 2015.

[3] Priyanka H., Gouri S. P.,"A Combined Approach of Steganography and Cryptography Techniques for Information Security: A Survey", International Journal of Engineering Research & Technology (IJERT) Vol. 4, Issue 12, December-2015.

[4] Mitali V. K., Arvind S.," A Survey on Various Cryptography Techniques", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 3, Issue 4, July-August 2014.

[5] Abdelmgeid A. A., Al – Hussien S. S.," Enhancing the Security of SMMWB Image Steganography Technique by using the Linked List Structure (Cover Package Method)", International Journal of Computer Applications (0975 – 8887) Volume 90 – No 7, March 2014.

[6] Pardeshi, S. M., Sonawane, I. R., Punjabi, V. D., & Saraf, P. A.," A Survey on compound use of Cryptography and Steganoghaphy for Secure Data Hiding", International Journal of Emerging Technology and Advanced Engineering Website, Volume 3, Issue 10, October 2013.

[7] Pujar, J. H., & Kadlaskar, L. M." A New Lossless Method of Image Compression and Decompression Using Huffman Coding Techniques." Journal of Theoretical & Applied Information Technology, Vol. 15, Issue 1/2, pp.18-23, 2010.

[8] Wa'el Ibrahim A. Al-Mazaydeh," Image Steganography using LSB and LSB+Huffman Code", International Journal of Computer Applications (0975 – 8887) Volume 99-No.5, August 2014.

[9] Varsha, Rajender S.," Data Hiding Using Steganography and Cryptography" International Journal of Computer Science and Mobile Computing, Vol.4 Issue.4, pp. 802-805, April- 2015.

[10] Tahir A. and Amit D." A Novel Approach of LSB Based Steganography Using Parity Checker" International Journal of Advanced Research in Computer Science and Software Engineering, Vol 5, Issue 1, January 2015.

[11] Yamuna D., Preethi. P.," A Secure Image Steganography Based on RSA Algorithm and Random Pixel Selection Technique", International Journal of Research in Engineering Technology and Management Vol. 03 Issue 03, May-2015.

[12] Marwa M. E., Abdelmgeid A. A., Fatma A. O. "A Modified Image Steganography Method based on LSB Technique." International Journal of Computer Applications, Vol. 125, No. 5, September 2015.

[13] Ajit S., Swati M., "Securing Data by Using Cryptography with Steganography", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013.

[14] Abdelmged A. A., Al-Hussien S. S., Nada H.," A Technique of Image Steganography using ParityChecker and LSBraille." International Journal of Computer Applications (0975 – 8887), Vol. 144 – No.4, June 2016.

[15] Usha, S., Kumar, G. S., Boopathybagan, K. "A secure triple level encryption method using cryptography and steganography." 20II International Conference on Computer Science and Network Technology *(ICCSNT)*, Vol. 2, pp. 1017-1020, December-2011).

[16] Rasha H.A., Sawsan H. J." Hiding Secret Text In Image Using Rc4 And Rijindeal Algorithm."International Journal of Computer Engineering and Technology (IJCET), ISSN 0976-6367, ISSN 0976 - 6375, Vol. 6, Issue 1, pp. 12-18, January (2015).

[17] Vijaypal D., Ramesh C. P., Yash V. S. "A Novel

Algorithm for Image Steganography Based on Effective Channel Selection Technique" International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, Issue 8, August 2013.

[18] Kamal D. "Relative Antropy Based Analysis of Image Steganography Techniques". International Journal of P2P Network Trends and Technology (IJPTT). Vol 1, Issue 3 - 2011.

[19] Abdelmged A.A, Shaimaa M.H,"New Image Steganography Method Using Zero Order Hold Zooming "International Journal of Computer Applications (0975 – 8887) Vol. 59–No.15, January 2016.

[20] Abdelmgeid A. A., Al – Hussien S. S.," New Technique for Encoding the Secret Message to Enhance the Performance of MSLDIP Image Steganography Method (MPK Encoding)", International Journal of Computer Applications (0975 – 8887) Vol. 59– No.15, December 2012.