International Conference on Information Engineering, Management and Security
2015 [ICIEMS 2015]

ISBN	978-81-929742-7-9
Website	www.iciems.in
Received	10 - July - 2015
Article ID	ICIEMS025

VOL	01
eMail	iciems@asdf.res.in
Accepted	31- July - 2015
eAID	ICIEMS.2015.025

An Optimize Utilization of Carrier Channels for Secure Data Transmission, Retrieval and Storage in Distributed Cloud Network using Key Management with Genetic Algorithm: A Review

Dr.C.A.Dhote[1], Mr.Virendra P.Nikam[2]
[1]Professor,Badnera College of Engineering,Badnera
[2]Phd Scholar

Abstract: *Relay transmission can enhance coverage and throughput, whereas it can be vulnerable to eavesdropping attacks due to the additional transmission of the source message at the relay. Thus, whether or not one should use relay transmission for secure communication is an interesting and important problem. In this paper, we consider the transmission of a confidential message from a source to a destination in a decentralized wireless network in the presence of randomly distributed eavesdroppers. The source–destination pair can be potentially assisted by randomly distributed relays. For an arbitrary relay, we derive exact expressions of secure connection probability for both colluding and nonpolluting eavesdroppers. We further obtain lower bound expressions on the secure connection probability, which are accurate when the eavesdropper density is small. Using these lower bound expressions, we propose a relay selection strategy to improve the secure connection probability. By analytically comparing the secure connection probability for direct transmission and relay transmission, we address the important problem of whether or not to relay and discuss the condition for relay transmission in terms of the relay density and source–destination distance. These analytical results are accurate in the small eavesdropper density regime.*

Keywords: Attack effect, low-rate distributed denial of service (DDoS) attack, mathematical model, and shrew attack.

INTRODUCTION

The power grid has become a necessity in the modern society. Without a stable and reliable power grid, tens of millions of people's daily life will be degraded dramatically [1] . For instance, the India blackout in July 2012 affected more than 60 million people (about 9% of the world population) and plunged 20 of Indian 28 states into darkness [2]. Indeed, the traditional power grid, which is surprisingly still grounded on the design more than 100 years ago, can no longer be suitable for today's society [3] With the development of information system and communication technology, Many countries have been modernizing the aging power system into smart grid, which is featured with two-way transmission, high reliability, real-time demand response, self-healing, and security. Within smart grid, Advanced Metering Infrastructure (AMI) plays a vital role and is associated with people's daily life most closely [4] . AMI modernizes the electricity metering system by replacing old mechanical meters with smart meters, which provide two-way communications between utility companies and energy customers. With the AMI, people can not only read the meter data remotely, but also do some customized control and implement fine-coarse demand 106 Tsinghua Science and Technology, April 2014, 19(2):

Cite this article as: Dr.C.A.Dhote, Mr.Virendra P.Nikam. "An Optimize Utilization of Carrier Channels for Secure Data Transmission, Retrieval and Storage in Distributed Cloud Network using Key Management with Genetic Algorithm: A Review." *International Conference on Information Engineering, Management and Security (2015)*: 152-158. Print.

105-120 Response [5]. In addition, the real-time data collected from the smart meters can improve the reliability of the distribution grid by avoiding line congestion and generation overloads [6].

The utility companies can also provide faster diagnosis of outage and dynamical electricity price thanks to the AMI. Hence, AMI has attracted great attention from many stakeholders, including utility companies, energy markets, regulators,etc. AMI technologies are rapidly overtaking the traditional meter reading technologies and millions of smart meters are equipped in the household all over the world. For example, there are already more than 4.7million smart meters used for billing and other purposes in Ontario, Canada[7] According to the American Institute for Electric Efficiency (IEE), approximately 36 million smart meters have been installed in the United State by May 2012, and additional 30 million smart meters will be deployed in the next three years [8]However, rich information exchange and hierarchical semi-open network structure in AMI extend the attack surface for metering to entire public networks and introduce many vulnerabilities for cyber attacks [9, 10] . Among all the attacks to the AMI, energy theft in emerging economies has been a widespread practice, both in developing countries and developed countries. A World Bank report finds that up to 50% of electricity in developing countries is acquired via theft [11] . It is reported that each year over 6 billion dollars are lost due to the energy theft in the United States alone [12]. In 2009, the FBI reported a wide and organized energy-theft attempt that may have cost up to 400 million dollars annually to a utility following an AMI deployment [13] . In Canada, BC Hydro reports $100 million in losses every year [14] . Utility companies in India and Brazil incur losses around $4.5 billion and $5 billion due to electricity theft, respectively [15, 16]. There is even a video which shows how to crack the meter and cut the electricity bill in half in Youtube [17] . As a result, energy-theft issue becomes one of the most important concerns which prohibit the development of AMI. Due to the nature of non-technical loss during transmission of electrical energy, it is very difficult for the utility companies to detect and fight the people responsible for energy theft. The unique challenges for energy theft in AMI call for the development of effective detection techniques. However, so far, few studies have elaborated what have been achieved and what should be done for these challenges. As a result,
we are motivated to investigate energy-theft issue in AMI, which is of critical importance to the design of AMI information networks and has been considered as one of the highest priorities for the smart grid design. In this paper, we provide a state-of-the-art survey of existing energy-theft detection schemes in AMI

LITERATURE SURVEY

Tung-Hsiang Liu and *Long-Wen Chang* [20] has proposed a simple data hiding technique for binary images in *2004*.The proposed method embeds secure data at the edge portion of host binary image. Binary images consist of only two colors therefore changing any pixels in this image could be easily detected by human eyes. Therefore, data is stored in the edge portion of binary image; as the modification of edge pixels is more difficult to be recognized by human eyes. The Distance matrix mechanism is used to find the edge pixels of host binary image. Then the Weight mechanism is used to consider the connectivity of the neighborhood around changeable pixels for choosing the most suitable one. For the security and quality consideration, a random number generator is used to distribute the embedding data into the overall image. This method not only embeds large amounts of data into host binary image but also can maintain image quality In order to improve the capacity of the hidden secret data and to provide am imperceptible stego image quality *H.-C. Wu, N.-I. Wu, C.-S. Tsai* and *M.-S. Hwang* [21] has proposed a novel stenographic method based on Least Significant Bit (LSB) Replacement and Pixel Value Differencing (PVD) methods in *2005*.Pixel Value Differencing (PVD) method is used to discriminate between edge areas and smooth areas of cover image. In Wu and Tsai's steganographic method, a grey-valued cover image is partitioned into non- overlapping blocks of two consecutive pixels, states pi and p_i and p_{i+1}.From each block we can obtain a different value d_i by subtracting pi from $p_{i+1.}$ All possible different values of d_i range from -255 to 255, then $|d_i|$ ranges from 0 to 255. Therefore, the pixel p_i and p_{i+1} are located within the smooth area when the value $|d_i|$ is smaller and will hide less secret data. Otherwise, it is located on the edged area and embeds more data. From the aspect of human vision it has a larger tolerance that embeds more data into edge areas than smooth areas. The secret data is hidden into the smooth areas of cover image by LSB method while using the PVD method in the edge areas. As, this proposed method not only store data in the edge areas but also in the smooth areas; therefore it can hide much larger information and maintains a good visual quality of stego image.

In *2005 M. Carli M.C.Q. Fariasy, E. Drelie Gelascaz, R. Tedesco &A. Neri* [22] has proposed a no-reference video quality metric that blindly estimates the quality of a video. They had used Block based Spread Spectrum embedding method to insert a fragile mark into perceptually important areas of the video frames. They used a set of perceptual features to characterize the perceptual importance of a region that are Motion, Contrast and Color. The mark is extracted from the perceptually important areas of the decoded video on receiver side. Then a quality measure of the video is obtained by computing the degradation of the extracted mark. So, in this way quality of a compressed video is estimated by using simple embedding system on perceptually important areas of the video frame.

In *2007 Hsien-Wen Tseng, Feng-Rong Wu*, and *Chi-Pin Hsieh* [23] has proposed a novel method for hiding data in binary images. The binary cover image is partitioned into equal-sized, non-overlapping blocks and the watermark will be embedded into blocks by flipping pixels. For security consideration, the watermark data is firstly permuted into a meaningless bit sequence by using a secret key. The cover image is partitioned into blocks of predefined size n x n and then each block can be embedded one secret bit except the completely black or white blocks. The embedding rule is based on the odd-even information in a block. A Weight mechanism is used to select the most suitable pixel for flipping. Additionally boundary check is performed to improve the visual quality of stego image as well as to prevent boundary distortion. This method achieved a good visual quality for watermarked image and has high capacity of embedding.

In *2008 Beenish Mehboob* and *Rashid Aziz Faruqui* [24] discussed the art and science of Steganography in general and proposed a novel technique to hide data in a colorful image using least significant bit. Least Significant Bit or its variants are used to hide data in digital image. Digital Images are represented in bits. The idea of playing with 0's and 1's seem quite simple but a slight change in value may transform an image completely ,in other words it distorts image completely. Therefore this technique chops the data in 8 bits after the header and used LSB to hide data. So, they proved LSB method is the most recommended for hiding data than other techniques which require masking and filtering.

M.B. Ould Medeniand &El Mamoun Souidi [25] has proposed a novel stenographic method for gray level images on four pixel differencing and LSB substitution in *2010*. The proposed approach works by dividing the cover into blocks of equal sizes and split each pixel into two parts .Then it counts number of one's in most part and embeds the secret message in the least part according to the corresponding number of bits in most part. As shown in following fig. 2.1

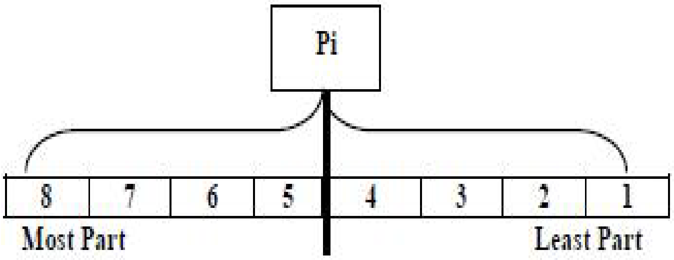

Figure 2.1: Split Process

$number-1-(MSB)$	$number-to-embeded$
$4or3$	$3bits$
2	$2bits$
$1or0$	1

TABLE: 2.1 Number of 1 and the Corresponding Number of Bits to Embed

Therefore, it embeds the message in the edge of the block depending on the number of ones in left four bits of the pixel. They used K-bit LSB substitution method for hiding the secret data into each pixel where K is decided by the number of one in the most part of pixel. This method gave best values for the PSNR measure which means that there were no big difference between the original and the stegno image.

In *2012 Tasnuva Mahjabin,Syed Monowar Hossain* and *Md. Shariful Haque* [26] has proposed a data hiding method based on PVD and LSB substitution to improve the capacity of the secret data as well as to make stegnalysis a complicated task they made an effort to implement a robust dynamic method of data hiding. An efficient and dynamic embedding algorithm was proposed here that not only hides secret data with an imperceptible visual quality and increased capacity but also make secret code breaking a good annoyance for the attacker. This method achieved an increased embedding capacity and lower image degradation with improved security as compared to LSB substitution method and some other existing methods of data hiding. This system used a dynamic method of image data hiding based on LSB Substitution method and Pixel Value Differencing method. The whole process of selecting eight pixels block for a sixteen pixels region and the embedding method for each eight pixels block is different for different cover images. That is, depending on the quality of the cover image the embedding procedure takes this decision in run time. This feature of this method provides security of the hidden secret data. In order to extract the secret data it is mandatory to know that the cover image is divided into regions of sixteen pixels and also the type of eight pixels block for these regions and type of method for each of these blocks. Moreover, if any one becomes aware of the techniques that have been used to insert data in one image, he cannot use the same technique to other images. For example, depending on the quality of the cover image the embedding technique can select horizontal block for inserting data in the first sixteen pixels region for one image whereas vertical eight pixels block for the other image. Thus the decision for steganalysis becomes difficult and this method becomes a secure one.

Ankit Chaudhary and *JaJdeep Vasavada* [27] has proposed an improved stenography approach for hiding text messages in RGB lossless images in *2012*.The security level is increased by randomly distributing the text message over the entire image *Ankit Chaudhary* and *JaJdeep Vasavada* [27] has proposed an improved stenography approach for hiding text messages in RGB lossless images in *2012*.The security level is increased by randomly distributing the text message over the entire image instead of clustering within specific image portions. The first step towards the random distribution of the message in image is using indicator values. They used MSB bits of Red, Green and Blue channel as pixel indicator values instead of utilizing an entire channel. The MSBs indicate in what sequence the message is hidden using the LSBs. In addition to this, this scheme is applied after applying compression to the original message; therefore it would be make it extremely difficult to break, even after suspicion of the message within an image. The scheme works as follows: The MSB remains unchanged when an LSB of a byte is utilized for storing a message. This scheme enables us to fully utilize all the LSBs of every channel of the cover image to store the hidden message and hence improve its capacity. Moreover the varying indicator values introduce a security aspect as it becomes increasingly difficult to decode the message even if its presence is suspected. They increased storage capacity by utilizing all the color channels for storing information and providing the source text message compression. The degradation of the images can be minimized by changing only one lease significant bitper color channel for hiding the message, incurring avery little change in the original image. So, this method increased the security level and improved the storage capacity while incurring minimal quality degradation.

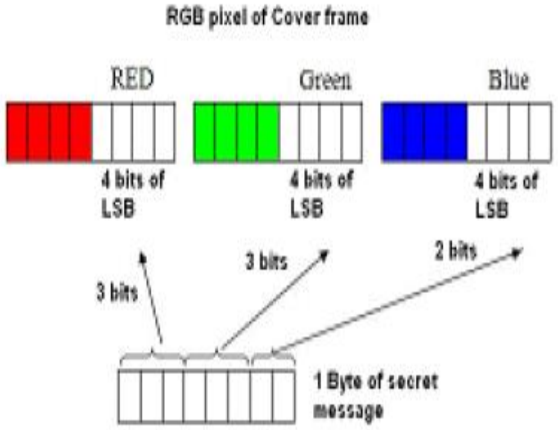

Figure: 2.2 shows secret data embedded in 4 bits of LSB in 3, 3, 2 order in corresponding RGB pixels of carrier frame

A hash function is used to select the position of insertion in LSB bits. The proposed technique takes eight bits of secret data at a time and conceal them in LSB of RGB (Red, Green and Blue) pixel value of the carrier frames in 3, 3, 2 order respectively. Such that out of eight (08) bits of message six (06) bits are inserted in R and G pixel and remaining two (02) bits are inserted in B pixel. After comparing the proposed technique with LSB technique it is found that the performance analysis of proposed technique is quite encouraging. The advantage of this method is that the size of the message does not matter in video stenography as the message can be embedded in multiple frames.

In *2012 Poonam V Bodhak* and *Baisa L Gunjal* [29] has proposed a method to hide data containing text in computer video file and to retrieve the hidden information. This can be designed by embedding the text file in a video file in such a way that the video does not lose its functionality using DCT & LSB Modification method. LSB is the lowest bit in a series of numbers in binary. The LSB based Steganography is one of the steganographic methods, used to embed the secret data in to the least significant bits of the pixel values in a cover image. DCT coefficients are used for JPEG compression. It separates the image into parts of differing importance. It transforms a signal or image from the spatial domain to the frequency domain. It can separate the image into high, middle and low frequency components.This method applies imperceptible modification. This proposed method strives for high security to an eavesdropper's inability to detect hidden information.
RigDas and *Themrichon Tuithung* [30] have proposed novel technique for image stenography based on Huffman Encoding in *2012*. Huffman Encoding is performed over the secret image/message before embedding and each bit of Huffman code of secret Image/message is embedded inside the cover image by altering the least significant bit (LSB) of each of the pixel's intensities of cover image. This paper presents a novel technique for image steganography based on Huffman Encoding. Two 8 bit gray level image of size M X N and P X Q are used as cover image and secret image respectively. As shown in fig: 2.3

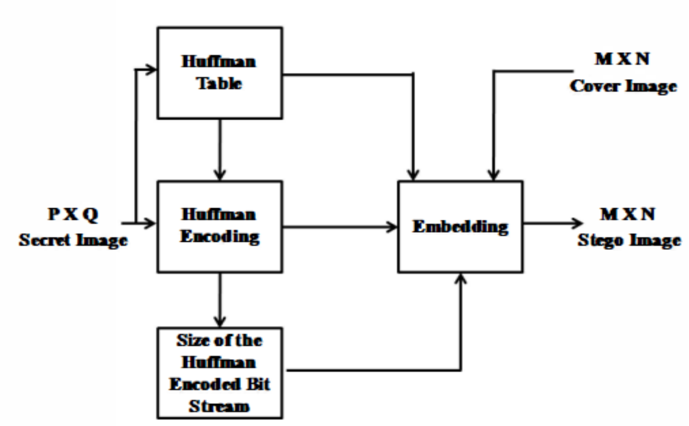

Figure: 2.3 Insertion of the Secret Image/Message into a Cover Image

Cite this article as: Dr.C.A.Dhote, Mr.Virendra P.Nikam. "An Optimize Utilization of Carrier Channels for Secure Data Transmission, Retrieval and Storage in Distributed Cloud Network using Key Management with Genetic Algorithm: A Review." *International Conference on Information Engineering, Management and Security (2015)*: 152-158. Print.

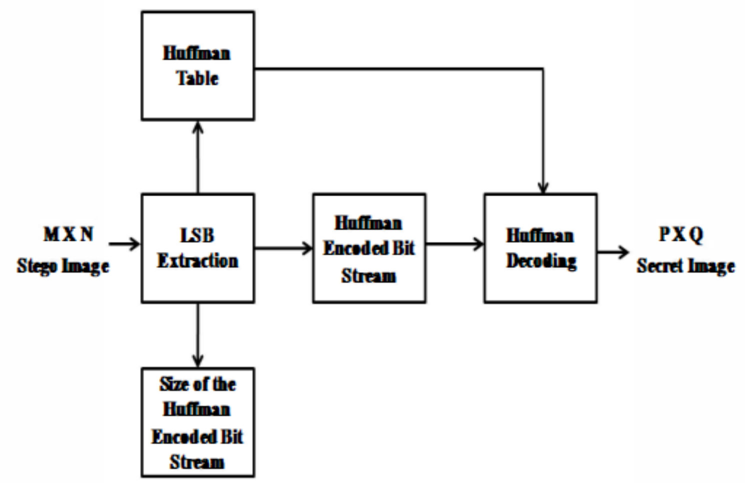

Figure: 2.4 Extraction of the Secret Image from the Stego Image

Huffman Encoding is performed over the secret image/message before embedding and each bit of Huffman code of secret image/message is embedded inside the cover image by altering the least significant bit (LSB) of each of the pixel's intensities of cover image. The size of the Huffman encoded bit stream and Huffman Table are also embedded inside the cover image, so that the Stego-Image becomes standalone information to the receiver.

In *2013 Ming Li,Michel K. Kulhandjian, Dimitris,A. Pados,,Stella N. Batalama,* and *Michael J. Medley* [31] has considered the problem of extracting blindly data embedded over a wide band in a spectrum (transform) domain of a digital medium (image, audio, video).We develop a novel multicarrier/signature iterative generalized least-squares (M-IGLS) core procedure to seek unknown data hidden in hosts via multicarrier spread-spectrum embedding. Neither the original host nor the embedding carriers are assumed available.

SUMMARY & DISCUSSION

Year	Author	Advantages
2004	Tung-Hsiang Liu Long-Wen Chang	Large amount of data can be stored in binary images as well as quality of an image is maintained.
2005	H.-C. Wu, N.-I. Wu, C.-S. Tsai M.-S. Hwang	Much larger information can be stored in images by using LSB method for storing data in smooth areas of image.
2005	M. Carli M.C.Q. Fariasy, E. Drelie Gelascaz, R. Tedesco, A. Neri	Quality of a compressed video is estimated by using simple embedding system.
2007	Hsien-Wen Tseng, Feng-Rong Wu,Chi-Pin Hsieh	This method achieved a good visual quality for watermarked image and has high capacity of embedding.

2010	M.B. Ould Medeni El Mamoun Souidi	K-bit LSB substitution method used here gave best values for the PSNR measure.
2012	Tasnuva Mahjabin, Syed Monowar Hossain Md.Shariful Haque	PVD & LSB methods used here which achieved an increased embedding capacity and lower image degradation with improved security.
2012	Ankit Chaudhary JaJdeep Vasavada	1-bit LSB substitution method used which increased the security level and improved the storage capacity
2012	Kousik Dasgupta, J.K.Mandal Paramartha Dutta	It allows embedding the large size of data in multiple frames. Therefore size of the message does not matter.
2012	Poonam V Bodhak Baisa L Gunjal	DCT & LSB methods used which provide high security to embedded data.
2012	RigDas ThemrichonTuithung	Huffman Encoding is used for secret message which again improves the security level of hiding data.
2013	Ming Li, Michel K. Kulhandjian, Dimitris, A. Pados, Stella N. Batalama, Michael J. Medley	M-IGLS procedure is used for extracting blindly data embedded over a wide band in a spectrum domain of a digital medium.

References:

[1] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, “Information hiding: A survey,” *Proc. IEEE, Special Issue on Identification and Protection of Multimedia Information*, vol. 87, no. 7, pp. 1062–1078, Jul.1999.

[2] I. J. Cox, M. L. Miller, and J. A. Bloom, *Digital Watermarking*. San Francisco, CA, USA: Morgan-Kaufmann, 2002.

[3] F. Hartung and M. Kutter, “Multimedia watermarking techniques,” *Proc. IEEE, Special Issue on Identification and Protection of Multimedia Information*, vol. 87, pp. 1079–1107, Jul. 1999

[4] G. C.Langelaar, I. Setyawan, and R. L. Lagendijk, “Watermarking digital image and video data: A state-of-the-art overview,” *IEEE Signal Process. Mag.*, vol. 17, no. 5, pp. 20–46, Sep. 2000.

[5] N. F. Johnson and S. Katzenbeisser, , S. Katzenbeisser and F. Petitcolas, Eds., “A survey of steganographic techniques,” in *Information Hiding*. Norwood, MA, USA: Artech House, 2000, pp. 43–78.

[6] S. Wang and H. Wang, “Cyber warfare: Steganography vs. steganalysis,” *Commun. ACM*, vol. 47, pp. 76–82, Oct. 2004.

[7] C. Cachin, “An information-theoretic model for steganography,” in *Proc. 2nd Int. Workshop on Information Hiding*,Portland, OR, USA, Apr. 1998, pp. 306–318.

Cite this article as: Dr.C.A.Dhote, Mr.Virendra P.Nikam. “An Optimize Utilization of Carrier Channels for Secure Data Transmission, Retrieval and Storage in Distributed Cloud Network using Key Management with Genetic Algorithm: A Review.” *International Conference on Information Engineering, Management and Security (2015)*: 152-158. Print.

[8] G. J. Simmons, “The prisoner’s problem and the subliminal channel,” in *Advances in Cryptology: Proc. CRYPTO’83*, New York, NY, USA, 1984, pp. 51–67, Plenum.

[9] J. Fridrich*, Steganography in Digital Media, Principles, Algorithms, and Applications*. Cambridge, U.K.: Cambridge Univ. Press, 2010.

[10] Y. Wang and P. Moulin, “Perfectly secure steganography: Capacity, error exponents, and code constructions,” IEEE *Trans. Inf. Theory*, vol. 54, no. 6, pp. 2706–2722, Jun. 2008.

[11] Federal Plan for Cyber Security and Information Assurance Research and Development Interagency Working Group on Cyber Security and Information Assurance, Apr. 2006.

[12] H. S.Malvar and D. A. Florencio, “Improved spread spectrum: A new modulation technique for robust watermarking,” *IEEE Trans. Signal Proc.*, vol. 51, no. 4, pp. 898–905, Apr. 2003.

[13] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shannon, “Secure spread spectrum watermarking for multimedia,” *IEEE Trans. Image Process.*, vol. 6, no. 12, pp. 1673–1687, Dec. 1997.

[14] J. Hernandez, M. Amado, and F. Perez-Gonzalez, “DCT-domain watermarking techniques for still images: Detector performance analysis and a new structure,” *IEEE Trans. Image Process.*, vol. 9, no. 1, pp.55–68, Jan. 2000

[15] C. Qiang and T. S. Huang, “An additive approach to transform-domain information hiding and optimum detection structure,” *IEEE Trans. Multimedia*, vol. 3, no. 3, pp. 273–284, Sep. 2001.

[16] C. Fei, D. Kundur, and R. H. Kwong, “Analysis and design of watermarking algorithms for improved resistance to compression,” *IEEE Trans. Image Process.*, vol. 13, no. 2, pp. 126–144, Feb. 2004.

[17] M. Gkizeli, D. A. Pados, and M. J. Medley, “SINR, bit error rate,and Shannon capacity optimized spread-spectrum steganography,” in *Proc. IEEE Int. Conf. Image Proce. (ICIP)*, Singapore, Oct. 2004, pp. 1561–1564.

[18]M. Gkizeli, D. A. Pados, S. N. Batalama, andM. J.Medley, “Blind iterativerecovery of spread-spectrum steganographic messages,” in *Proc. IEEE Int. Conf. Image Proc. (ICIP)*, Genova, Italy, Sep. 2005, vol. 2,pp. 11–14.

[19] M. Gkizeli, D. A. Pados, and M. J. Medley, “Optimal signature design for spread-spectrum steganography,” *IEEE Trans. Image Process.*, vol. 16, no. 2, pp. 391–405, Feb. 2007.

[20] Tung-Hsiang Liu and Long-Wen Chang, “An Adaptive Data Hiding Technique for Binary Images”, *Proc.IEEE 17th Int.Conf. On Pattern Recognition (ICPR’04)* 2004.

[21]H.-C. Wu, N.-I. Wu, C.-S. Tsai and M.-S. Hwang,” Image steganographic scheme based on pixel-value differencing and LSB replacement methods”, *IEE Proc.-Vis. Image Signal Process*., Vol. 152, No. 5, October 2005.

[22] M. Carli , M.C.Q. Fariasy, E. Drelie Gelascaz, R. Tedesco, A. Neri, “QUALITY ASSESSMENT USING DATA HIDING ON PERCEPTUALLY IMPORTANT” *IEEE* AREAS0-7803-9134-9/05/$20.00 ©2005.

[23]Hsien-Wen Tseng, Feng-Rong Wu,and Chi-Pin Hsieh,” Data Hiding for Binary Images Using Weight Mechanism”,*IEEE* 2007.

[24]Beenish Mehboob and Rashid Aziz Faruqui,” A StegnographyImplementation”, *IEEE* 2008

[25] M.B. Ould MEDENI, El Mamoun SOUIDI,” A Novel Steganographic Method for Gray-Level Images With four-pixel Differencing and LSB Substitution “*IEEE* 2010

[26] Tasnuva Mahjabin, Syed Monowar Hossain, Md. Shariful Haque,” A Block Based Data Hiding Method in Images Using Pixel Value Differencing and LSB Substitution Method”, *IEEE* 2012.

[27] Ankit Chaudhary, JaJdeep Vasavada,”A Hash Based Approach for Secure Keyless Image Steganography in Lossless RGB Images”, *IEEE* 2012.

Cite this article as: Dr.C.A.Dhote, Mr.Virendra P.Nikam. “An Optimize Utilization of Carrier Channels for Secure Data Transmission, Retrieval and Storage in Distributed Cloud Network using Key Management with Genetic Algorithm: A Review.” *International Conference on Information Engineering, Management and Security (2015)*: 152-158. Print.