IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-6, Issue-7, July 2018 E-ISSN: 2347-2693

Analysis on LSB based detection methods and hiding strategies with color images

A.K. Chaturvedi[1*], Annu Sharma[2], Kalpana Sharma[3]

[1] MCA Deptt, Govt. Engineering College, Ajmer, India
[2] CSE Deptt., Bhagwant Univ., Ajmer, India
[3] CSE Deptt., Bhagwant Univ., Ajmer, India

[*]*Corresponding Author: amit0581@gmail.com, Tel.: 9829265881*

Available online at: www.ijcseonline.org

Accepted: 13/Jul/2018, Published: 31/July/2018

***Abstract*—** The internet users are regularly increasing day by day. After the launching of the 4G or IMT-Advanced services, communication over internet increased drastically. People across all the communities like social, economical, business, financial, etc are doing communication or exchanging their valued documents over internet. Hence, the demand of securing these documents or hiding some secret message into another cover is also increased. As, Steganography is the art and science of hiding a secret message in another message, image, or video as cover, in such a way, which hides the existence of the communication. Its goal is to hide messages inside other harmless messages, or image and does not allow any enemy to even detect that there is a second message present. In this paper, we have presented an analysis on LSB based detection methods and current hiding strategies with color images. Many noticeable hiding strategies proposed by researchers are presented here, but more research is required with the objectives of achieving high embedding payload and less detectable against the modern detector SPAM.

***Keywords*—** Secret Message, Data Hiding, Steganography, Detection Method, Color Images, SPAM.

I. INTRODUCTION

Steganography supports different types of digital formats that are used for hiding the data. These files are known as carriers. Depending upon the redundancy of the object, suitable formats are used. Redundancy is the process of providing better accuracy for the object that is used for display by the bits of object. The main file formats that are used for steganography are Text, images, audio and video. Steganography is also used for the less dramatic purpose of watermarking. The applications of watermarking mainly involve the protection of intellectual property such as ownership protection, file duplication management, document authentication (by inserting an appropriate digital signature) and file annotation. A larger part of steganalysis works published so far deals with grayscale and color images. Note that there are two aspects of steganalysis. The first relates to the attempt to break or attack a steganography; the second uses it as an effective way of evaluating and measuring steganography security performance.

Information hiding can achieve the functions of covert communication and copyright protection and so on. LSB information hiding is one of the significant methods of information hiding. It if proposed firstly by A.Z Tirkel in 1993 [1]. Various steganography techniques have been proposed in literature. The Least Significant Bit (LSB) steganography is one such technique in which least significant bit of the image is replaced with data bit. As this method is vulnerable to steganalysis, so as to make it more secure and encrypt the raw data before embedding it in the image. Though the encryption process increases the time complexity, but at the same time provides higher security also.

Image steganography is widely used for hiding information in the cover image, because this is quite simple and secure way to transfer the information over the internet. Steganography can be used in a large amount of data formats in the digital world of today. The most popular data formats are .bmp, .doc, .gif, .jpeg, .mp3, .txt and .wav. Steganographic technology is a very important part of the future of Internet security and privacy on open systems such as Internet.

II. RELATED WORK

Quantum computation has the ability to solve some problems that are considered inefficient in classical computer. Research on Quantum image processing has been extensively exploited in recent decades. Quantum image information hiding can be divided into quantum image digital

© 2018, IJCSE All Rights Reserved

watermarking, quantum image steganography, anonymity and other branches. Least significant bit (LSB) information hiding plays an important role in classical world because many information hiding algorithms are designed based on it. In this paper, based on novel enhanced quantum representation (NEQR), the concrete least significant qubit (LSQb) information hiding algorithm for quantum image is given firstly. Because information hiding located on the frequency domain of an image can increase the security, we further discuss the frequency domain LSQb information hiding algorithm for quantum image based on quantum Fourier transform. In our algorithms, the corresponding unitary transformations are designed to realize the aim of embedding the secret information to the least significant qubit representing color of the quantum cover image. Finally, we illustrate the procedure of extracting the secret information. Quantum image LSQb information hiding algorithm can be applied in many fields according to different needs [2].

Image steganography is a growing research field, where sensitive contents are embedded in images, keeping their visual quality intact. Researchers have used correlated color space such as RGB, where modification to one channel affects the overall quality of stego-images, hence decreasing its suitability for steganographic algorithms. Therefore, in this paper, we propose an adaptive LSB substitution method using uncorrelated color space, increasing the property of imperceptibility while minimizing the chances of detection by the human vision system. In the proposed scheme, the input image is passed through an image scrambler, resulting in an encrypted image, preserving the privacy of image contents, and then converted to HSV color space for further processing. The secret contents are encrypted using an iterative magic matrix encryption algorithm (IMMEA) for better security, producing the cipher contents. An adaptive LSB substitution method is then used to embed the encrypted data inside the V-plane of HSV color model based on secret key-directed block magic LSB mechanism. The idea of utilizing HSV color space for data hiding is inspired from its properties including de-correlation, cost-effectiveness in processing, better stego image quality, and suitability for steganography as verified by our experiments, compared to other color spaces such as RGB, YCbCr, HSI, and Lab. The quantitative and qualitative experimental results of the proposed framework and its application for addressing the security and privacy of visual contents in online social networks (OSNs), confirm its effectiveness in contrast to state-of-the-art methods [3].

In this paper, we propose a novel robust blind color image watermarking method, namely SMLE, that allows to embed a gray-scale image as watermark into a host color image in the wavelet domain. After decomposing the gray-scale watermark to component binary images in digits ordering from least significant bit (LSB) to most significant bit (MSB), the retrieved binary bits are then embedded into wavelet blocks of two optimal color chan- nels by using an efficient quantization technique, where the wavelet coefficient difference in each block is quantized to either two pre-defined thresholds for corresponding 0-bits and 1-bits. To optimize the watermark imperceptibility, we equally split the coefficient modified quantity on two middle-frequency sub-bands instead of only one as in existing approaches. The improvement of embedding rule increases approximately 3 dB of water- marked image quality. An adequate trade-offbetween robustness and imperceptibility is controlled by a factor representing the embedding strength. As for extraction process, we exploit 2D Otsu algorithm for higher accuracy of watermark detection than that of 1D Otsu. Experimental results prove the robustness of our SMLE watermarking model against com- mon image processing operations along with its efficient retention of the imperceptibility of the watermark in the host image. Compared to state-of-the-art methods, our approach outperforms in most of robustness tests at a same high payload capacity [4].

In this paper, a novel steganographic method is proposed employing an immune programming strategy to find a near-optimal solution for the pair-wise least-significant-bit (LSB) matching scheme. The LSB matching method proposed by Mielikaien utilizes a binary function to reduce the number of changed pixel values. However, his method still has room for improvement. A tier-score system is proposed in this paper to assess the performance of different orders for LSB matching. An immune programming approach is adopted to search for a near-optimal solution among all the permutation orders. The proposed method can reduce the distortion of the stego image, improve the visual quality, and decrease the probability of detection. The experimental results show that the proposed method achieves better performance than Mielikainen's pair-wise LSB matching method in terms of distortion and survival probability against steganalysis [5].

Data hiding in encrypted image is a hot topic of data security in recent years. In this paper, we propose a reversible data hiding algorithm with high capacity in encrypted domain by exploiting alpha channel of portable network graphics (PNG) image. Specifically, our algorithm divides secret data into some segments. For each segment, one bit is embedded into the LSB of encrypted pixel and other bits are hidden in the corresponding element of the alpha channel, which is finally encrypted by two chaotic maps. With the use of alpha channel, our algorithm can perfectly recover secret data and reach high embedding capacity and good visual quality. Many experiments with standard benchmark images are carried out to validate efficiency of our algorithm. Comparison shows that our algorithm outperforms Zhang's algorithm [6].

In this paper, we present a novel, reversible steganographic method, which can reconstruct an original image effectively

© 2018, IJCSE All Rights Reserved

after extracting the embedded secret data. The proposed reversible hiding method aims at BTC (block truncation coding)-compressed color images. Conventionally, each block of a color image compressed by BTC requires three bitmaps and three pairs of quantization levels for reconstruction. In order to improve the compression rate, a genetic algorithm (GA) is applied to find an approximate optimal common bitmap to replace the original three. The secret data then are embedded in the common bitmap and the quantization levels of each block use the properties of side matching and the order of these quantization levels to achieve reversibility. The experimental results demonstrate that the proposed method is practical for BTC-compressed color images and can embed more than three bits in each BTC-encoded block on average [7].

In this paper, we proposed a novel method to embed a series of ternary secret data into a cover image based on an improved Least-Significant-Bit (LSB) scheme using the modulo three strategy. Our new method can hide two ternary numbers into each grayscale pixel, normally only modify the two LSBs of the pixel, while it may cause overflow/underflow and a carry/borrow. We solve these problems by adding 1 to the pixel or subtracting 1 from the pixel before embedding. The embedding capacity of our method can be 3.1699 bpp. At the same time, the quality of the stego image of our new method also is better than traditional LSB scheme when the embedding capacity is greater than 3 bpp with a Peak Signal-to-Noise Ratio (PSNR) greater than 37 dB. Extensive experimental results indicated that our new method is capable of getting a higher PSNR than traditional LSB scheme when the embedding capacity is greater than 3 bpp, and it has higher resistance ability against the chosen steganalysis algorithm when the embedding capacity is low [8].

Chuan Qin, Ping Ji, Xinpeng Zhang , Jing Dong, Jinwei Wang proposed a new fragile watermarking scheme with high-quality recovery capability based on overlapping embedding strategy. The block-wise mechanism for tampering localization and the pixel- wise mechanism for content recovery are collaborated in the proposed scheme. With the assist of inter- leaving operation, reference bits are derived from mean value of each overlapping block, and then are dispersedly embedded into 1 LSB or 2 LSB layers of the image, corresponding to horizontal-vertical mode and diagonal mode, respectively. Authentication bits are hidden into adaptive LSB layers of the central pixel for each block according to block complexity. On the receiver side, after locating tampered blocks and reconstructing mean-value bits, according to the types of tampered pixels in each overlapping block, three pixel-wise manners are exploited for tampering recovery based on different neighboring blocks. Even if the tampered area is extensive, the proposed scheme can achieve better quality of recovered im- age compared with some of state-of-the-art schemes [9].

Daniel Lerch-Hostalot, David Megıas presented a novel method for detection of LSB matching steganography in grayscale images. This method is based on the analysis of the differences between neighboring pixels before and after random data embedding. In natural images, there is a strong correlation between adjacent pixels. This correlation is disturbed by LSB matching generating new types of correlations. The presented method generates patterns from these correlations and analyzes their variation when random data are hidden. The experiments performed for two different image databases show that the method yields better classification accuracy compared to prior art for both LSB matching and HUGO steganography. In addition, although the method is designed for the spatial domain, some experiments show its applicability also for detecting JPEG steganography [10].

HayatAl-Dmour,AhmedAl-Ani, presented a novel image steganography algorithm that combines the strengths of edge detection and XOR coding, to conceal a secret message either in the spatial domain or an Integer Wavelet Transform (IWT) based transform domain of the cover image. Edge detection enables the identification of sharp edges in the cover image that when embedding in would cause less degradation to the image quality compared to embedding in a pre-specified set of pixels that do not differentiate between sharp and smooth areas. This is motivated by the fact that the human visual system (HVS) is less sensitive to changes in sharp contrast are as compared to uniform are as of the image. The edge detection method presented here is capable of estimating the exact edge intensities for both the cover and stego images (before and after embedding the message), which is essential when extracting the message. The XOR coding, on the other hand, is a simple, yet effective, process that helps in reducing differences between the cover and stego images. In order to embed three secret message bits, the algorithm requires four bits of the cover image, but due to the coding mechanism, no more than two of the four bits will be changed when producing the stego image. The proposed method utilizes the sharpest regions of the image first and then gradually moves to the less sharp regions. Experimental results demonstrate that the proposed method has achieved better imperceptibility results than other popular steganography methods. Furthermore, when applying a textural feature steganalytic algorithm to differentiate between cover and stego images produced using various embedding rates, the proposed method maintained a good level of security compared to other steganography methods [11].

B. Feng, J. Weng, Wei Lu, Bei Pei proposes a steganalytic scheme to detect recently developed content adaptive binary image data hiding by exploiting the embedding effect associated with the l-shape pattern-based embedding criterion. We first assess how changing l-shape patterns affects the distribution of a special 4 x 3 sized pattern. Based

© 2018, IJCSE All Rights Reserved

on the assessment, 4 classes of patterns that model the distribution of two pixels oriented the direction of pattern changing are employed to define a 32-dimensional steganalytic feature set. Experimental results show that, despite of the low dimensionality, the proposed steganalytic features can effectively detect state-of-the-art binary image data hiding schemes, especially those pattern-tracing-based approaches [12].

B. B. Haghighi, A. H. Taherinia, A. Harati proposed a fragile and blind dual watermarking method for tamper detection and self-recovery. This method generates two image digests from the host image, based on the lifting wavelet and the halftoning technique. Therefore, for each 2× 2 non-overlapping blocks, two chances for recovering tampered blocks is provided. Then, the authentication bit is obtained by using the image digests. Totally, eight bits are embedded in two LSBs for each block of image. To enhance the quality of the digest, a new LSBRounding technique is proposed. Additionally, to determine the mapping blocks and shuffling LSBs, the Arnold Cat Map is utilized. To improve the recovery rate, a Shift-aside operation is proposed. For preventing copy-move, vector-quantization attacks, and any manipulation in LSBs, the information embedded in each block depends on the key which is assigned to it. Experimental results show the efficiency of TRLH compared to the state of the art methods [13].

S. Sajasi, A.M. E. Moghadam presents an irreversible scheme for hiding a secret image in the cover image that is able to improve both the visual quality and the security of the stego-image while still providing a large embedding capacity. This is achieved by a hybrid steganography scheme incorporates Noise Visibility Function (NVF) and an optimal chaotic based encryption scheme. In the embedding process, first to reduce the image distortion and to increase the embedding capacity, the payload of each region of the cover image is determined dynamically according to NVF. NVF analyzes the local image properties to identify the complex areas where more secret bits should be embedded. This ensures to maintain a high visual quality of the stego-image as well as a large embedding capacity. Second, the security of the secret image is brought about by an optimal chaotic based encryption scheme to transform the secret image into an encrypted image. Third, the optimal chaotic based encryption scheme is achieved by using a hybrid optimization of Particle Swarm Optimization (PSO) and Genetic Algorithm (GA) which is allowing us to find an optimal secret key. The optimal secret key is able to encrypt the secret image so as the rate of changes after embedding process be decreased which results in increasing the quality of the stego-image. In the extracting process, the secret image can be extracted from the stego-image losslessly without referring to the original cover image. The experimental results confirm that the proposed scheme not only has the ability to achieve a good trade-off between the payload and the stego-image quality, but also can resist against the statistics and image processing attacks [14].

A three-phase intelligent technique has been constructed to improve the data-hiding algorithm in colour images with imperceptibility. The first phase of the learning system (LS) has been applied in advance, whereas the other phases have been applied after the hiding process. The first phase has been constructed to estimate the number of bits to be hidden at each pixel (NBH); this phase is based on adaptive neural networks with an adaptive genetic algorithm using upwind adaptive relaxation (LSANN-AGAUpAR1). The LS of the second phase (LSANN-AGAUpAR2) has been introduced as a detector to check the performance of the proposed steganographic algorithm by creating a rich images model from available cover and stego images. The LS of the last phase (LSCANN-AGAUpAR3) has been implemented through three steps, and it is based on a concurrent approach to improve the stego image and defend against attacks. The adaptive image filtering and adaptive image segmentation algorithms have been introduced to randomly hide a compressed and encrypted secret message into a cover image. The NBH for each pixel has been estimated cautiously using 32 principle situations (PS) with their 6 branch situations (BS). These situations have been worked through seven layers of security to augment protection from attacks. In this paper, hiding algorithms have been produced to fight three types of attacks: visual, structural, and statistical attacks. The simulation results have been discussed and compared with new literature using data hiding algorithms for colour images. The results of the proposed algorithm can efficiently embed a large quantity of data, up to 12 bpp (bits per pixel), with better image quality [15].

This paper introduces a new technique to increase the information security over the network using steganography in such a way that the secret message being sent is unidentifiable. There is a comparison made to give a clear view of how the algorithm proposed is better than LSB algorithm which is used since a long time for sending concealed messages. To avoid the chances of an attacker using steganalysis to retrieve the data, the data encryption is done. S-tool is used to show the reliability of this algorithm. We will be comparing both LSB and DKL algorithms on the basis of Mean Square Error, Peak Signal Noise Ratio, Relative Payload and Rate of Embedding. Here by its shown that DKL algorithm is more efficient than LSB algorithm [16].

Two techniques BLOWFISH algorithm for cryptography and LSB approach for stagnography are used. First encryption of data is done by using BLOWFISH algorithm which is one of the most powerful techniques and then hide encrypted message using LSB approach. Our proposed model gives two layers of security for secret data [17].

© 2018, IJCSE All Rights Reserved

Amit and Jyoti presented a review on image steganography security issues, like complexity, and general overview of cryptography and digital watermarking approaches. Also it provides deepness discussions of stenographic algorithms like Least Significant Bit (LSB) algorithm. It also compares those algorithms in terms of speed, accuracy and security to enhance the concept of steganography. It also offers a chance to put the theory into practice by way of a piece of software designed to maximize learning in the fields. This paper gives a brief idea about the image steganography that make use of Least Significant Bit (LSB) algorithm for hiding the data into image [18].

III. LEAST SIGNIFICANT BIT (LSB) INSERTION METHOD

The least significant bit insertion method is probably the most well-known image steganography technique. It is a common, simple approach to embedding information in a graphical image file. Unfortunately, it is extremely vulnerable to attacks, such as image manipulation. A simple conversion from a GIF or BMP format to a lossy compression format such as JPEG can destroy the hidden information in the image.

When applying LSB techniques to each byte of a 24-bit image, three bits can be encoded into each pixel. (As each pixel is represented by three bytes.) Any changes in the pixel bits will be indiscernible to the human eye. For example, the letter A can be hidden in three pixels. Assume the original three pixels are represented by the three 24-bit words below:

(00100111 11101001 11001000)

(00100111 11001000 11101001)

(11001000 00100111 11101001)

The binary value for the letter A is (10000011). Inserting the binary value of A into the three pixels, starting from the top left byte, would result in

(00100111 11101000 11001000)

(00100110 11001000 11101000)

(11001000 00100111 11101001)

The emphasised bits are the only bits that actually changed. The main advantage of LSB insertion is that data can be hidden in the least and second to least bits and still the human eye would be unable to notice it. When using LSB techniques on 8-bit images, more care needs to be taken, as 8-bit formats are not as forgiving to data changes as 24-bit formats are. Care needs to be taken in the selection of the cover image, so that changes to the data will not be visible in the stego-image. Commonly known images, (such as famous paintings, like the Mona Lisa) should be avoided. In fact, a simple picture of your dog would be quite sufficient.

When modifying the LSB bits in 8-bit images, the pointers to entries in the palette are changed. It is important to remember that a change of even one bit could mean the difference between a shade of red and a shade of blue. Such a change would be immediately noticeable on the displayed image, and is thus unacceptable. For this reason, data-hiding experts recommend using grey-scale palettes, where the differences between shades is not as pronounced [19].

IV. HIDING STRATEGIES

Research on hiding secret messages in the image cover is going on and many information or data hiding strategies are proposed. Some of the noticeable contributions are listed here. K. Muhammad, M. Sajjad, I. Mehmood, S. Rho, and S.W.Baik proposed an adaptive LSB substitution method using uncorrelated color space, increasing the property of imperceptibility while minimizing the chances of detection by the human vision system [3]. Thien Huynh-The , Cam-Hao Hua , Nguyen Anh Tu and their team proposed a novel robust blind color image watermarking method, namely SMLE, that allows to embed a gray-scale image as watermark into a host color image in the wavelet domain. After decomposing the gray-scale watermark to component binary images in digits ordering from least significant bit (LSB) to most significant bit (MSB), the retrieved binary bits are then embedded into wavelet blocks of two optimal color chan- nels by using an efficient quantization technique, where the wavelet coefficient difference in each block is quantized to either two pre-defined thresholds for corresponding 0-bits and 1-bits.

H. Xu, J. Wang, H.J. Kim proposed a novel steganographic method is proposed employing an immune programming strategy to find a near-optimal solution for the pair-wise least-significant-bit (LSB) matching scheme. Chin-Chen Chang, Chih-Yang Lin, and Yi-Hsuan Fan proposed a novel, reversible steganographic method, which can reconstruct an original image effectively after extracting the embedded secret data. The proposed reversible hiding method aims at BTC (block truncation coding)-compressed color images. W.L.Xu, C.C. Chang, T.S. Chen, L.M.Wang proposed a novel method to embed a series of ternary secret data into a cover image based on an improved Least-Significant-Bit (LSB) scheme using the modulo three strategy. Our new method can hide two ternary numbers into each grayscale pixel, normally only modify the two LSBs of the pixel, while it may cause overflow/underflow and a carry/borrow. We solve these problems by adding 1 to the pixel or subtracting 1 from the pixel before embedding. These are some of the strategies that may be used for data or information hiding using LSB steganography. Every strategy have some benefits and drawbacks also.

© 2018, IJCSE All Rights Reserved

V. CONCLUSION

The LSB modification technique provides an easy way to embed information in images, but the data can be easily decoded. Certainly the time complexity of the overall process increases but at the same time the security achieved at this cost is well worth it. LSB and MSB steganography techniques are gaining more popularity than other techniques.

New approaches are still a subject for the research in this field with the objectives of achieving high embedding payload and less detectable against the modern detector SPAM.

ACKNOWLEDGMENT

The authors are thankful to all the people, who help or encourage us directly or indirectly, for the preparation of this research paper..

REFERENCES

[1] G. Shailender and A.G. Bhushan, "Information Hiding least significant bit steganography and cryptography", Int.Journal of Education and Computer Science, vol. 6, 2012, pp. 27-34

[2] S. Wang, J. Sang, X. Song, X. Niu, "Least Significant Qubit (LSQb) Information Hiding Algorithm for Quantum Image", Elsevier, Measurement (2015), doi: http://dx.doi.org/10.1016/j.measurement. 2015.05.038

[3] K. Muhammad, M. Sajjad, I. Mehmood, S. Rho, S. W. Baik, "Image steganography using uncorrelated color space and its application for security of visual contents in online social networks", Future Generation Computer Systems 86 (2018), pp. 951–960

[4] Thien Huynh-The , Cam-Hao Hua , N. Anh Tu , Taeho Hur , J. Bang , D. Kim , M. Bilal Amin, B. Ho Kang , H. Seung , S. Lee, "Selective bit emb e dding scheme for robust blind color image watermarking", Elsevier, Info. Sciences 426 (2018),pp. 1–18

[5] Huan Xu, Jianjun Wang, Hyoung Joong Kim, Near-optimal solution to pair-wise LSB matching via an immune programming strategy, Elsevier, Information Sciences 180 (2010), pp. 1201–121

[6] Zhenjun Tang, Quanfeng Lu, Huan Lao, Chunqiang Yu, Xianquan Zhang, Error-free reversible data hiding with high capacity in encrypted image, Elsevier, Optik, Vol. 157 (2018), pp. 750–760

[7] Chin-Chen Chang, Chih-Yang Lin, Yi-Hsuan Fan, Lossless data hiding for color images based on block truncation coding, Elsevier, ScienceDirect, Pattern Recognition, vol. 41 (2008), pp. 2347 – 2357

[8] Wen-Long Xu, Chin-Chen Chang, Tung-Shou Chen, Liang-Min Wang, "An improved least-significant-bit substitution method using the modulo three strategy", Elsevier, ScienceDirect, Displays vol. 42 (2016), pp. 36–42

[9] Chuan Qin, Ping Ji, Xinpeng Zhang , Jing Dong, Jinwei Wang, "Fragile image watermarking with pixel-wise recovery based on overlapping emb e dding strategy", Elsevier, Signal Processing, vol. 138 (2017), pp. 280–293

[10] Daniel Lerch-Hostalot, David Megıas," LSB matching steganalysis based on patterns of pixel differences and random embedding", Elsevier, computers & security, vol. 32 (2013), pp. 192-206.

[11] HayatAl-Dmour,AhmedAl-Ani, "A steganography embedding method based on edge identification and XOR coding", Elsevier, Expert SystemsWithApplications, vol. 46(2016), pp. 293–306

[12] B. Feng, J. Weng, Wei Lu, Bei Pei, "Steganalysis of content-adaptive binary image data hiding", Elsevier, J. Vis. Commun. Image R. vol. 46 (2017), pp. 119–127

[13] B. B. Haghighi, A. H. Taherinia, A. Harati, "TRLH: Fragile and blind dual watermarking for image tamper detection and self-recovery based on lifting wavelet transform and halftoning technique", Elsevier, Journal of Visual Communication and Image Representation, vol 50 (2018), pp. 49–64

[14] S. Sajasi, A.M. E. Moghadam, "An adaptive image steganographic scheme based on Noise Visibility Function and an optimal chaotic based encryption method", Elsevier, Applied Soft Computing, vol. 30 (2015), pp. 375–389

[15] N. N. El-Emama, M. Al-Diabat, "A novel algorithm for colour image steganography using a new intelligent technique based on three phases", Elsevier, Applied Soft Computing, vol. 37 (2015), pp. 830–846

[16] S. Udhayavene, A. T. Dev and K. Chandrasekaran, "New Data Hiding Technique In Encrypted Image: DKL Algorithm (Differing Key Length)", Elservier, Procedia Computer Science, vol. 54 (2015), pp. 790 – 798, Eleventh International Multi-Conference on Information Processing-2015 (IMCIP-2015)

[17] K. Patel, S. Utareja, H. Gupta, "Information Hiding using Least Significant Bit Steganography and Blowfish Algorithm", International Journal of Computer Applications (0975 – 8887), Volume 63– No.13, February 2013, pp. 24-28

[18] Amit and Jyoti, "REVIEW OF INFORMATION HIDING USING LEAST SIGNIFICANT BIT STEGANOGRAPHY IN BMP & JPG IMAGES", ISSN 2319-5991, Vol. 3, No. 3, 2014, pp. 96-102

[19] Sabu M Thampi, "Information Hiding Techniques : A Tutorial Review", ISTE-STTP on Network Security & Cryptography, LBSCE 2004

Authors Profile

Dr. Amit Chaturvedi obtained the Ph.D. degree in Mar, 2012. He is presently teaching in the Govt. Engineering College, Ajmer. He has 17 years long PG teaching experience. Five doctorate degrees are awarded under his supervision. He has published around 72 research papers in national/international Journals and conference. He has written three text books in the computer science subjects. Presently he is working on the subjects of cloud computing and multicast communication in adhoc networks.

.

Mrs Anu Sharma, obtained the MCA degree in 2008 from MDS University, Ajmer, M.Phil from MJRP Univ., Jaipur in 2011 and have long experience in teaching. She is presently pursuing Ph.D. from Bhagwant University, Ajmer

© 2018, IJCSE All Rights Reserved