INTERNATIONAL JOURNAL OF EXPLORING EMERGING TRENDS IN ENGINEERING
Peer-Reviewed, Refereed, Indexed and International Journal, https://ijoeete.com/
|ISSN No. 2394-0573 |Volume: 10, Issue: 2 | July - Dec 2023

REVIEW OF LITERATURE LSB-BASED IMAGE STEGANOGRAPHY IN SECURE AND VERIFIABLE COLOR VISUAL CRYPTOGRAPHY

[1] Basawaraja, [2]Dr. Praveen Kumar
[1]Research Scholar, [2]Supervisor
[1-2] Department of Computer Science, SunRise University, Alwar, Rajasthan (India)

Abstract: Several Image Steganography techniques are in vogue, amongst which, Least Significant Bit (LSB) is a well known approach. It is used to embed the secret message/ data/ information within a cover image. Two famous sub techniques that can be covered under the umbrella of LSB are (i) Insertion based Method (ii) Substitution based Method. Both are widely adopted and used for hiding data but there are some differences between them. Insertion based method increases the size of the image when secret data is embedded while on other hand the substitution-based method is used to replace the bits of the image with secret data without increasing the size of the image

Keywords: REVIEW OF LITERATURE, LSB BASED IMAGE STEGANOGRAPHY, COLOR VISUAL CRYPTOGRAPHY

Introduction: Image steganography is a technique for embedding secret messages on an image as a storage medium. In the science of steganography, there is one important aspect, namely imperceptibility, this aspect means that the secret message must not be felt by the human sensory system[7–9]. Because the media in the form of images that appear visually, the human sense of sight is used as a benchmark. Please note that the human visual system is more sensitive to color images than grayscale images[6], this means the methods proposed in grayscale images and have been proven good, still need to be tested again on color images to ensure the results

G. Prashanti and K. Sandhyarani have done survey on recent achievements of LSB based image steganography. In this survey authors discuss the improvements that enhance the steganographic results such as high robustness, high embedding capacity and un-detectability of hidden information. Along with this survey two new techniques are also proposed. First technique is used to embed data or secret messages into the cover image and in the second technique a secret gray scale image is embedded into another gray scale image. These techniques use four state table that produce pseudo random numbers. This is used for embedding the secret information.

One method of steganography in digital images that have long been used is the least significant bit (LSB). Although this method is still very popular and continues to be used today. This method works in the spatial domain, which is the process of embedding messages directly by manipulating the smallest bit value of pixels[10,11]. LSB also has advantages in the aspect of imperceptibility and has a relatively large message storage capacity. In previous research conducted by Astuti et al. [12] stated that the LSB-based bit flipping method can increase the imperceptibility of a stego image of around 9dB if measured by the PSNR measurement tool. The 9dB difference is a great value and contributes well to the imperceptibility aspect, but in testing the method still uses grayscale imagery. The bit flipping method is a technique used to change the message bit value with the negation value of the bit. Bit flipping is done when the cover image bit changes by more than 50%. In digital image storage systems on computers generally use red, green, and blue (RGB) color formats. The RGB color format has a depth of 24 bits, where each color layer has 8 bits [13]. In the RGB color format, the spread of the intensity is relatively equal on each color layer, which intensity is the energy carried on a digital image [6]. This study discusses the analysis of the effect of the method of flipping bits on color images with the LSB-based RGB format

Review of Literature

On the based on Huffman Coding, Amitava Nag et al. [7] present a novel steganographic technique of LSB substitution. Their technique basically focuses on high security, larger embedding capacity and acceptable level of stego image quality. Firstly Huffman tree is produced to encode every 8 bits of secret image. After encoding, they divide the encoded bits into four parts and have 0 to 3 decimal values. Location of embedding a message in cover image is determined by these decimal values. Experimental results show that it is very difficult for attacker to extract the secret information because Huffman table decrease the size of the cover image. Purposed techniques just have acceptable level of PSNR values and lie between 30 dB to 31 dB. 2014: N. Akhtar et al. in [8] present and implement the improved version of traditional LSB image steganography technique. Their work enhances the quality of stego image using bit inversion method. They propose and implement two approaches of bit inversion techniques. These both techniques resolves around bit inversion techniques in which LSBs of pixels of carrier image are inverted only and only if they arise with specific pattern of pixel's bits. This leads to lesser modification in pixels is compared to traditional LSB method. For correct retrieval of secret message, inverted bits need to be embedded somewhere within

the stego image. Experimental results demonstrate that PSNR value of stego image is improved; hence stego image quality is improved.

G. Prashanti and K. Sandhyarani [4] have done survey on recent achievements of LSB based image steganography. In this survey authors discuss the improvements that enhance the steganographic results such as high robustness, high embedding capacity and un-detectability of hidden information. Along with this survey two new techniques are also proposed. First technique is used to embed data or secret messages into the cover image and in the second technique a secret gray scale image is embedded into another gray scale image. These techniques use four state table that produce pseudo random numbers. This is used for embedding the secret information. These two methods have greater security because secret information is hidden on random selected locations of LSBs of the image with the help of pseudo random numbers generated by the table.

Naor and Shamir generalized basic secrete sharing scheme into k out of n visual cryptography scheme [1]. In k out of n visual cryptography scheme, n shares of the original image are generated and given to n participant. Minimum k of those n participant have to provide theirs share for reveling the secrete image. Contrast of the recovered image is poor and pixel expansion is double in this scheme. To provide the security to this scheme, G. Ateniese et al. further modified (k, n) model to general access structure model of visual cryptography [2]. According to them number of share n, created are divided into two parts or subsets as per the importance and need. First part of the subset is called qualified subset and second is forbidden subset. Any k shares from qualified subset can recover the secret image. From the forbidden set k or more shares cannot recover the secret image. AbhishekParakh et.al.proposed “Recursive threshold visual cryptography” [3].

The basic idea behind Recursive threshold visual cryptography is recursive hiding of smaller secrets in shares of larger secrets with secret sizes doubling at every step, and thereby increasing the information, every bit of share conveys to (n-1)/n bit of secret which is nearly 100%again to maintain the good contrast and improve the security, Zhi Zhou, et.al. proposed halftone visual cryptography [4], [9].In halftone visual cryptography a secret binary pixel is encoded into an array of sub pixels, called as halftone cell, in each of the n shares. Mahmoud E. Hodeish et.al proposed an optimized half tone visual cryptography using error diffusion. They works on binary and gray scale image and improves the pixel expansion, elements the code book requirement but they only works on binary half tone images[6]. Mahmoud E. Hodeish et.al proposed a new efficient TKHC-based image sharing scheme over unsecured channel they proposed the method of RGB and gray scale images encrypted and decrypted by means of TKHC and providing strong security to transmit all the generated shares via one public channel [9]. Chang-Chou Lin et.al.proposed visual cryptography for gray level images [10].

Bingwen Feng, Wei Lu, and Wei Sun in their paper “Secure Binary Image Steganography Based on Minimizing the Distortion on the Texture” [8] purposed a stateof-the-art approach of binary image steganography. This technique is proposed to minimize the distortion on the texture. In this method of steganography firstly the rotation, complement and mirroring invariant texture patterns are extracted from the binary image. They also proposed a measurement and based on this proposed measurement this approach is practically implemented. Practical results show that proposed steganographic approach has high statistical security with high stego image quality and high embedding capacity.

2015: M. Nusrati et al. [18] have done study on heuristic genetic algorithm based steganographic method for hiding secret information in a cover image. This method optimally find the appropriate locations in cover image to embed the secret information by focusing on the “before embedding hiding techniques”. It tries to make least changes in the bits which lead to minimal modifications in image histogram. To covert the LSBs and secret message to set of blocks, segmentation is done in this genetic algorithm. After this algorithm finds the appropriate locations for embedding, the secret blocks are embedded and it generates the key file which is used during message extraction process. Experimental results show that this genetic based method is more efficient than basic LSB algorithm with high stego image quality.

The scheme uses the dithering technique for conversion of gray level image into approximate binary image. Then they have applied existing Visual cryptography schemes for binary images to create the shares. To reduces the pixel expansion F.Liu, etal. proposed a new approach for colored visual cryptography scheme [11]. They proposed three different approaches for color image representation in which they separate three color channels Red, green and blue. Any one channel can be used in half toning process but quality of image gets degraded due to half-toning process. Wang et al. [12] proposed the Sharing a Secret Image in Binary Images with Verification. In this scheme, it is difficult to manage and process the meaningless shares and it also consumes time to scramble the images.Kalyan Das et al. [20] suggested a novel visual secret sharing technique that is based on pixel intensity adjustment function and some basic binary operations for providing the confidentiality and integrity of the transmitted visual image. The scheme proposed by them provides time efficient solution.

2014-2015: Savita Goel et al. in [20] proposed a new method of embedding secret messages in cover image using LSB method using different progressions. Authors compare the quality of stego image with respect to cover image

using number of image quality parameters such as Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), histograms and CPU time, Structure Similarity (SSIM) index and Feature Similarity Index Measure (FSIM). Their study and experimental results shows that their proposed method is fast and highly efficient as compared to basic LSB methods. 2015: Della Baby et al. [19] proposed a "Novel DWT based Image Securing method using Steganography". In their work new steganography technique is prosed in which multiple RGB images are embedded into single RGB image using DWT steganographic technique. The cover image is divided into 3 colors i.e. Red, Green and Blue color space. These three color spaces are utilized to hide secret information. Experimental results obtained using 2 this system has good robustness. Value of PSNR and SSIM index have been used by authors to compare the quality of stego image and original cover image. Proposed method has good level of PSNR and SSIM index values. Authors have found that their experimental results are better than existing approaches and have increased embedding capacity because of data compression. So overall security of their approach is high with less perceptible changes in stego image.

References:

1. Pawar, S.S., Kakde, V.: Review on steganography for hiding data. Int. J. Comput. Sci. Mob. Comput. **4**, 225–229 (2014)

2. Muhammad, K., Ahmad, J., Rho, S., Baik, S.W.: Image steganography for authenticity of visual contents in social networks. Multimed. Tools Appl. **76**, 18985–19004 (2017)

3. Islam, M.R., Siddiqa, A., Uddin, M.P., Mandal, A.K., Hossain, M.D.: An efficient filtering-based approach improving LSB image steganography using status bit along with AES cryptography. In: 2014 International Conference on Informatics, Electronics and Vision (ICIEV), pp. 1–6. IEEE Press, New York (2014)

4. Odat, A.M., Otair, M.A.: Image steganography using modified least significant bit. Indian J. Sci. Technol. **9**, 1–5 (2016)

5. Li, B., He, J., Huang, J., Shi, Y.Q.: A survey on image steganography and steganalysis. J. Inf. Hiding Multimed. Sig. Process. **2**, 142–172 (2011)

6. Akhtar, N., Johri, P., Khan, S.: Enhancing the security and quality of LSB based image steganography. In: 2013 5th International Conference and Computational Intelligence and Communication Networks, pp. 385–390. IEEE Press, New York (2013)

7. Muhammad, K., Ahmad, J., Farman, H., Zubair, M.: A novel image steganographic approach for hiding text in color images using HSI color model. Middle-East J. Sci. Res. **22**, 647–654 (2014)

8. Cheddad, A., Condell, J., Curran, K., Mc Kevitt, P.: Digital image steganography: survey and analysis of current methods. Sig. Process. **90**, 727–752 (2010)

9. Samima, S., Roy, R., Changder, S.: Secure key-based image realization steganography. In: 2013 IEEE Second International Conference on Image Information Processing (ICIIP-2013), pp. 377–382. IEEE Press, New York (2013)

10. Tilakaratne, U.T., Pinidiyaarachchi, U.A.J.: Image steganography scheme based on reversible data embedding strategy. In: 8th International Conference on Computer Science and Education (ICCSE), pp. 503–507. IEEE Press, New York (2013)

11. Thenmozhi, S., Chandrasekaran, M.: A novel technique for image steganography using nonlinear chaotic map. In: 2013 7th International Conference on Intelligent Systems and Control (ISCO), pp. 307–311. IEEE Press, New York (2013)

12. Jan, Z., Mirza, A.M.: Genetic programming-based perceptual shaping of a digital watermark in the wavelet domain using Morton scanning. J. Chin. Inst. Eng. **35**, 85–99 (2012)

13. Wang, S., Sang, J., Song, X., Niu, X.: Least significant qubit (LSQb) information hiding algorithm for quantum image. Measurement **73**, 352–359 (2015)

14. Thai, T.H., Retraint, F., Cogranne, R.: Statistical detection of data hidden in least significant bits of clipped images. Sig. Process. **98**, 263–274 (2014)

15. Al-Shatnawi, A.M., Bader, M.A.: An integrated image steganography system with improved image quality. Appl. Math. Sci. **7**, 3545–3553 (2013)

16. Liu, Q., Sung, A.H., Ribeiro, B., Wei, M., Chen, Z., Xu, J.: Image complexity and feature mining for steganalysis of least significant bit matching steganography. Inf. Sci. **178**, 21–36 (2008)

17. Xu, W.L., Chang, C.C., Chen, T.S., Wang, L.M.: An improved least-significant-bit substitution method using the modulo three strategy. Displays **42**, 36–42 (2016)

18. Mao, Q.: A fast algorithm for matrix embedding steganography. Dig. Sig. Process. **25**, 248–254 (2014)

19. Nagaraj, V., Vijayalakshmi, V., Zayaraz, G.: Color image steganography based on pixel value modification method using modulus function. IERI Procedia **4**, 17–24 (2013)

20. Biswas, D., Biswas, S., Majumder, A., Sarkar, D., Sinha, D., Chowdhury, A., Das, S.K.: Digital image steganography using dithering technique. Procedia Technol. **4**, 251–255 (2012)