An image steganography approach based on k-least significant bits (k-LSB)

Omar Elharrouss, Noor Almaadeed, Somaya Al-Maadeed
Department of Computer Science and Engineering
Qatar University
Doha, Qatar

***Abstract*—Image steganography is the operation of hiding a message into a cover image. the message can be text, codes, or image. Hiding an image into another is the proposed approach in this paper. Based on LSB coding, a k-LSB-based method is proposed using k least bits to hide the image. For decoding the hidden image, a region detection operation is used to know the blocks contains the hidden image. The resolution of stego image can be affected, for that, an image quality enhancement method is used to enhance the image resolution. To demonstrate the effectiveness of the proposed approach, we compare it with some of the state-of-the-art methods.**

***Index Terms*—Image steganography, LSB , k-LSB, Entropy filter.**

I. Introduction

Steganography is a secret communication technique when the messages between to edge are encrypted and no one can detect the existence of hidden messages except the sender and the receiver of the message [1]. Before the digital images, the secret communication was made using manuscript letters of a list of numbers that can be referred to any other thing like a book or street numbers.

Recently, information hiding techniques have become an important practice in wide areas and applications, including digital images [3], digital audio, and video [2] [5] [6] [4]. The military communications systems employ a high level of traffic security techniques which instead of just hiding the message content by the encryption process; it seeks to existence [7]. The information hiding refers to two concepts steganography and digital watermarking. The steganography is defined as the attempt to hide the fact that information is being transmitted in the first place, while watermarking is usually referred to as the involved methods by which an identified information is being hidden in a data object, and accordingly, the information will be kept robust against modification [8]. Steganography is considered a kind of a hidden communication which means literally the "covered writing". Originally, it has been derived from the two Greek words stegano which refers to "covered" and graphos which refers to "to write". The goal of applying the steganography is to hide the information message inside a harmless cover medium in a certain way that makes it impossible to detect the secret information and even its existence in the cover medium [9]. Secrete information hiding is a method of steganography that works by hiding secrete information into digital images for the purpose of identification, annotation, and copyrighting. In fact, several constraints affect such a process and this is including, the quantity of the proposed data to be hidden, the need for invariance of these data under conditions where a "host" signal is subjected to distortions, e.g., lossy compression, in addition to the degree to which the data must be immune to an interception, a modification, or a removal by a third party [10]. Generally, steganography requires high security and capacity levels, i.e. hidden information is usually a fragile one which can be destroyed by even slight modifications. On the other hand, watermarking mostly relies on achieving a robustness status where it is impossible to remove the watermark without causing severe cover content quality degradation [11].

The rest of the paper is organized as follows. The literature overview related to our work are presented in section 2. The proposed system is presented in section 3. Experimental analysis is provided in section 4. The conclusion and future works are given in section 5.

II. Related works

The image becomes the most used feature in multimedia and in people's life [12]. The importance of images and the simplicity of transferring and sharing between people make the use of daily. The images are used also for hiding any information including text, numbers, images inside [13]. Many image steganography methods have been proposed. Classical least significant bit (LSB) is the classical method used for hiding any information in an image [14]. Especially on digital images, LSB represents one of the most used ways for hiding information based on digital characteristics and many proposed approaches are based on this technique [15]. Nowadays image steganography methods focus on the use of quantum images LSB-based [16] [17]. For hiding a message into an image, LBS based algorithm consist of replacing the last three bits of the cover image pixels with each up to three bits of the message data values that need to be hidden [18] [19]. But when we hide more data into an image by using LSB, it induces more noise hence image resolution (Quality of image) changed at the pixels where the data is hidden and

978-1-7281-4821-2/20/$31.00 ©2020 IEEE

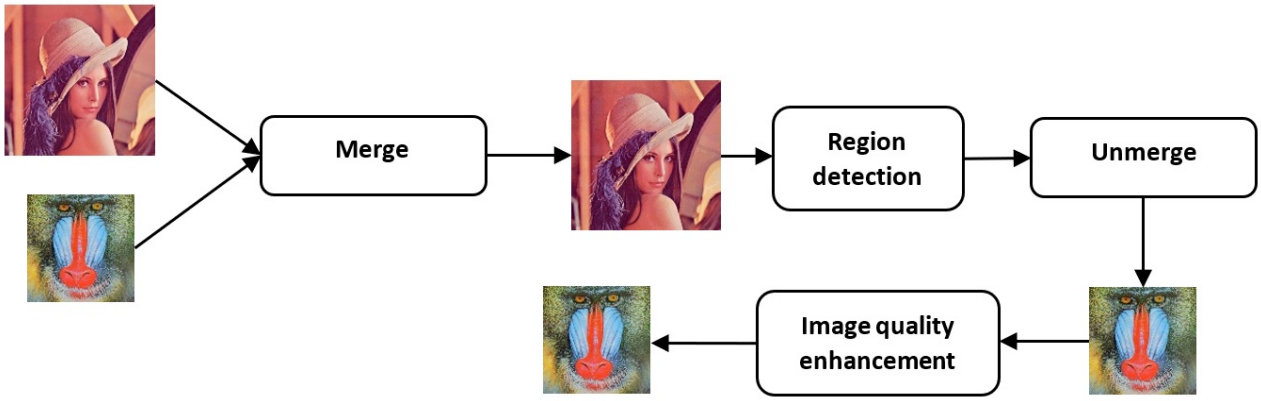

Fig. 1. Proposed method for pose categorization.

the security of information is less as someone can detect the message by recovering the least significant bit of the pixels from the image [20] [21].

Other techniques are used without using LSB algorithm. The authors in [23] proposed an image steganography method based on burst errors and STCs decoding damage. the existence of an embedded message, the authors verify it using proposed techniques using Poisson distribution. Image steganography on medical images was proposed in [24] based on the dependencies of inter-block coefficients. On binary images and using a proposed distortion measurement [25], as well as in [27] using the same technique. Based on amplifying channel modification probabilities on RGB images the authors attempt to handle the payload partition problems [26]. An Edge Based Image Steganography method is proposed in [28]. To generate stego images with good visual quality eth authors in [29] use pixel density and a novel construction called pixel density histogram (PDH) for image steganography. Based on object detection and relationship mapping the authors proposed an image steganography algorithm [30]. Using Local Binary Pattern (LBP) the authors proposed a method for image steganography [31]. The description of the feature used allows transmission of the secret information. The pair swapping with human visual system (HVS) model is used for the image steganography method in [32]. For more detail, a work provided an image steganography review in [33].

III. Proposed method

Image steganography is the operation of hiding a message into a cover image. the message can be text, codes, or image. Hiding an image into another is the proposed approach in this paper. Based on LSB coding, a k-LSB-based method is proposed using k least bits to hide the image. For decoding the hidden image, a region detection operation is used to know the blocks contains the hidden image. The resolution of stego image can be affected, for that, an image quality enhancement method is used to enhance the image resolution.

The simplest technique used in Image steganography is the LSB-based algorithm. The researcher uses it to embed a text message into a cover image using the three least significant bits. But in order to embed an image into an image, the three least three bits are not sufficient. The four first bits of a pixel can be for representing the content of the pixel. For that, in this paper, we follow this to hide an image into another. The quality of the cover images, as well as the stego images, can be affected. For that, we use an image quality enhancement algorithm after extracting the embedded image. the operation of extraction of the stego image is based on the same techniques as the encoding part which consists of extracting the least four-bit of each pixel channel. By the following, we describe the proposed embedding technique in detail. Figure 1 represents the flowchart of the proposed approach. The basic LSB approach is given by:

$$I = \{I_{ij}/0 \leq i < M, 0 \leq j < N\} \ where \ I_{ij} \in \{0, 1, 2, ..., 255\} \quad (1)$$

$$C_t(p) = \{c_i/1 \leq i < t, c_i \in \{0, 1\}\} \quad (2)$$

$$C_t(I + H) = \left\{\sum_{t=1}^{4} c_t(I_{ij}) \sum_{t=5}^{8} c_t(H_{ij})\right\} \quad (3)$$

A. Region detection with entropy-based local image descriptor

in order to detect the region that contains the hidden image, local entropy filter is used. As in [34], the entropy filter is difined, using a given image with L gray levels, by the follwong expression:

$$E(P0, P1, P2, ..., PL - 1) = -\sum_{i=0}^{L-1} P_i log P_i \quad (4)$$

The local entropy of a pixel in position q can be defined as:

$$e(q) = -\sum_{k=0}^{L-1} p_k log p_k \quad (5)$$

where p_k is the probability of gray level k appearing in the neighborhood Ω , and n_k is the number of pixels with gray level k in the neighborhood Ω . Hence, we use

(a) (b) (c) (d)

Fig. 2. Region detection results. (a) original image . (b) image to be hidden . (c) stego image . (d) entropy filter on stego image.

TABLE I
PSNR VALUES OF STEGO IMAGES

Image	**[17]**	**[31]**	**[22]**	**[20]**	**Ours**
Lena	56.533 (gray)	37	33.16	32.093	32.490
Airplane	-	37	32.74	–	32.774
Peppers	57.0953 (gray)	37	33.21	–	32.725
Baboon	56.0156 (gray)	37	32.41	–	32.448

a sliding window of size $m \times n$ (e.g. 9×9) to compute the local entropy.

Local image descriptors are necessary to appropriately guide the modulation of the filtering parameters across the image. Entropy-based image descriptors have already been used for edge detection, and adaptive filters based on local image content. We use the entropy-based image descriptor to guide the modulation of the range parameter. Figure 2 presents local entropy results applied to the image that contains the hidden images. the results images represent the local characteristics of an image.

B. *Image quality enhancement*

After extracting the hidden image, the resolution can be affected. For that and in order to enhance the image quality, the image quality enhancement method proposed in [35] is used. the method is based on the use of relative global histogram stretching (RGHS) based on adaptive parameter acquisition.

IV. Discussion

The effectiveness of the proposed method for hiding an image into another is evaluated by the metric peak signal-to-noise ratio (PSNR) .In steganography, when the secret data is embedded. PSNR measures the ratio of noise between the stego image and the original one. Based on the PSNR value, the image quality will be better when its value is higher.

Table 1 illustrates the evaluation of image steganography methods including the proposed method and the state-of-the-art methods including [17] [22]. for the PSNR values, we can observe that the proposed image steganography algorithm in [17] and [31] succeeds to hide the secret message in the images with a min modification in the images. the reason for this is that the authors hide some digit in the image, which represents a simple modification in the image. the image steganography method proposed in [22] hides some binary blocks in the images and this explains the PSNR values comparing with [17] and [31]. For the proposed method and the [20] that hides RGB image into another, the PSNR values are close to [22] even we are hiding RGB images which more complicated than a binary blocks.

In order to demonstrate the effectiveness of the proposed method, an evaluation using PSNR on the hidden image after extraction followed by enhancement of the image quality. Using the proposed method in which is used for enhancing the hidden images after extraction, Table 2 illustrates some results of enhancement on the same images.

Figure 3 presents some examples of hidden images with different sizes, also local entropy results applied to stego images that contain the hidden images. We can observe that the stego images in Figure 3 (c) contains some modified regions. the modified regions represent the position of the hidden images.

V. Conclusion

In this paper, an image steganography method has been presented for hiding an image into another. Using the k-LSB-based technique the proposed method start by merging the cover image and the images to be hidden. In order to detect the region that contains the hidden images, a region detection operation has been presented using the local entropy filter. Then, after extracting the hidden image, an image quality enhancement method has been applied in order to enhance the image that can bee affected during the hiding processes.from the experimental results, and using the evaluation metrics, the proposed method

TABLE II
PSNR VALUES OF EXTRATCED HIDDEN IMAGE BEFORE AND AFTER ENHANCEMENT

Cover image	Hidden image	Extracted image	PSNR-before	PSNR-after
Lena(512×512)	baboon(512×512)	baboon(512×512)	28.41	32.83
lena(512×512)	baboon(256×256)	baboon(256×256)	31.18	33.85

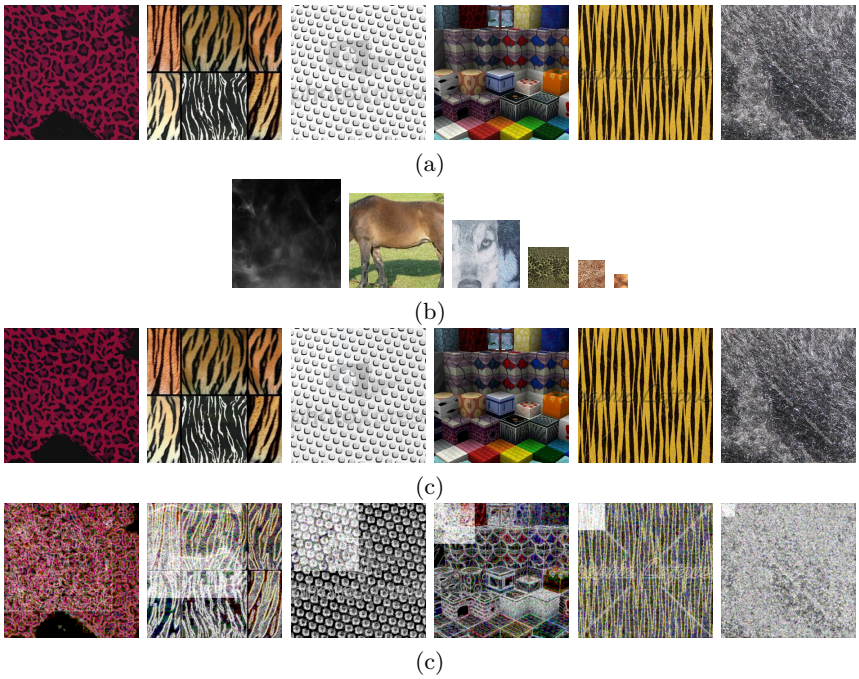

Fig. 3. Region detection results. (a) original images . (b) images to be hidden . (c) stego images . (d) entropy filter on stego images.

can hide the images and extract it with the minimum cost in term of distortion and the lose of information.

ACKNOWLEDGMENT

This publication was made by NPRP grant # NPRP 11S – 0113 – 180276 from the Qatar National Research Fund (a member of the Qatar Foundation). The statements made herein are solely the responsibility of the authors.

REFERENCES

[1] Tang, W., Li, B., Tan, S., Barni, M. and Huang, J., 2019. CNN-based adversarial embedding for image steganography. IEEE Transactions on Information Forensics and Security, 14(8), pp.2074-2087.

[2] Almaadeed, N., Elharrouss, O., Al-Maadeed, S., Bouridane, A. and Beghdadi, A., 2019. A Novel Approach for Robust Multi Human Action Detection and Recognition based on 3-Dimentional Convolutional Neural Networks. arXiv preprint arXiv:1907.11272.

[3] Elharrouss, O., Almaadeed, N., Al-Maadeed, S. and Akbari, Y., 2019. Image inpainting: A review. Neural Processing Letters, pp.1-22.

[4] Elharrouss, O., Almaadeed, N. and Al-Maadeed, S., 2020. MHAD: Multi-Human Action Dataset. In Fourth International Congress on Information and Communication Technology (pp. 333-341). Springer, Singapore.

[5] Abbad, A., Elharrouss, O., Abbad, K. and Tairi, H., 2018. Application of MEEMD in post-processing of dimensionality reduction methods for face recognition. IET Biometrics, 8(1), pp.59-68.

[6] Elharrouss, O., Moujahid, D. and Tairi, H., 2015. Motion detection based on the combining of the background subtraction and the structure–texture decomposition. Optik-International Journal for Light and Electron Optics, 126(24), pp.5992-5997.

[7] S.Arivazhagan, W.Sylvia Lilly Jebarani, and S.Bagavath (2011) "Colour Image Steganography Using Median Maintenance", ICTACT Journal on Image and Video Processing, Vol. 2, Iss:01, pp.246- 253.

[8] Sathishkumar GA,Ramachandran S, Bagan KB. (2012) Encrypt Image using random pixel permutation by chaotic mapping. In IEEE symposium on computers & informatics (pp. 247-51).

[9] Hemalatha.S, U.Dinesh Acharya , (2013) "Comparison of Secure and High Capacity Color Image Steganography Techniques in RGB and YCBCR domains", International Journal of Advanced Information Technology, Vol.3, No.3, pp.1-9.

[10] Praneeta Dehare, Padma Bonde (2014) "Hiding Image in Image by using FMM with LSB Substitution in Image Steganography ", International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169 Volume: 2 Issue: 11,pp 3663 – 3667.

[11] Jiang, N., Zhao, N. and Wang, L., 2016. LSB based quantum image steganography algorithm. International Journal of Theoretical Physics, 55(1), pp.107-123.

[12] Mahmood, A. and Al-Maadeed, S., 2019. Action recognition in poor-quality spectator crowd videos using head distribution-based person segmentation. Machine Vision and Applications, pp.1-14.

[13] Elharrouss, O., Al-Maadeed, N. and Al-Maadeed, S., 2019, June.

Video Summarization based on Motion Detection for Surveillance Systems. In 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC) (pp. 366-371). IEEE.

[14] Fridrich, J. and Long, M., 2000, July. Steganalysis of LSB encoding in color images. In 2000 IEEE International Conference on Multimedia and Expo. ICME2000. Proceedings. Latest Advances in the Fast Changing World of Multimedia (Cat. No. 00TH8532) (Vol. 3, pp. 1279-1282). IEEE.

[15] Gupta, S., Gujral, G. and Aggarwal, N., 2012. Enhanced least significant bit algorithm for image steganography. IJCEM International Journal of Computational Engineering & Management, 15(4), pp.40-42.

[16] Wang, S., Sang, J., Song, X. and Niu, X., 2015. Least significant qubit (LSQb) information hiding algorithm for quantum image. Measurement, 73, pp.352-359.

[17] Qu, Z., Cheng, Z., Liu, W. and Wang, X., 2019. A novel quantum image steganography algorithm based on exploiting modification direction. Multimedia Tools and Applications, 78(7), pp.7981-8001.

[18] Singh, A. and Singh, H., 2015, March. An improved LSB based image steganography technique for RGB images. In 2015 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT) (pp. 1-4). IEEE

[19] Al-Afandy, K.A., Faragallah, O.S., ELmhalawy, A., El-Rabaie, E.S.M. and El-Banby, G.M., 2016, October. High security data hiding using image cropping and LSB least significant bit steganography. In 2016 4th IEEE International Colloquium on Information Science and Technology (CiSt) (pp. 400-404). IEEE.

[20] Patel, N. and Meena, S., 2016, November. LSB based image steganography using dynamic key cryptography. In 2016 International Conference on Emerging Trends in Communication Technologies (ETCT) (pp. 1-5). IEEE.

[21] Arya, A. and Soni, S., 2018. Performance Evaluation of Secrete Image Steganography Techniques Using Least Significant Bit (LSB) Method. vol, 6, pp.160-165.

[22] Swain, G., 2019. Very high capacity image steganography technique using quotient value differencing and LSB substitution. Arabian Journal for Science and Engineering, 44(4), pp.2995-3004.

[23] Zhang, Y., Qin, C., Zhang, W., Liu, F. and Luo, X., 2018. On the fault-tolerant performance for a class of robust image steganography. Signal Processing, 146, pp.99-111.

[24] Liao, X., Yin, J., Guo, S., Li, X. and Sangaiah, A.K., 2018. Medical JPEG image steganography based on preserving inter-block dependencies. Computers & Electrical Engineering, 67, pp.320-329.

[25] Zhang, J., Lu, W., Yin, X., Liu, W. and Yeung, Y., 2019. Binary image steganography based on joint distortion measurement. Journal of Visual Communication and Image Representation, 58, pp.600-605.

[26] Liao, X., Yu, Y., Li, B., Li, Z. and Qin, Z., 2019. A new payload partition strategy in color image steganography. IEEE Transactions on Circuits and Systems for Video Technology.

[27] Yeung, Y., Lu, W., Xue, Y., Huang, J. and Shi, Y.Q., 2019. Secure binary image steganography with distortion measurement based on prediction. IEEE Transactions on Circuits and Systems for Video Technology.

[28] Rashid, R.D. and Majeed, T.F., 2019, March. Edge Based Image Steganography: Problems and Solution. In 2019 International Conference on Communications, Signal Processing, and their Applications (ICCSPA) (pp. 1-5). IEEE.

[29] Lu, W., Xue, Y., Yeung, Y., Liu, H., Huang, J. and Shi, Y., 2019. Secure Halftone Image Steganography Based on Pixel Density Transition. IEEE Transactions on Dependable and Secure Computing.

[30] Meng, R., Zhou, Z., Cui, Q., Sun, X. and Yuan, C., 2019. A Novel Steganography Scheme Combining Coverless Information Hiding and Steganography. Joural of Information Hiding and Privarcy Protection, 1(1), pp.43-48.

[31] Qiu, A., Chen, X., Sun, X., Wang, S., Wei, G., Wang, P., Chen, T., Wang, Z., Sun, J., Li, Y. and Shen, Y., 2019. Coverless Image Steganography Method Based on Feature Selection.

[32] Liu, W., Yin, X., Lu, W., Zhang, J., Zeng, J., Shi, S. and Mao, M., 2020. Secure halftone image steganography with minimizing the distortion on pair swapping. Signal Processing, 167, p.107287.

[33] Sidqi, H.M. and Al-Ani, M.S., 2019. Image Steganography: Review Study. In Proceedings of the International Conference on Image Processing, Computer Vision, and Pattern Recognition (IPCV) (pp. 134-140). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

[34] Dai, T., Lu, W., Wang, W., Wang, J. and Xia, S.T., 2017. Entropy-based bilateral filtering with a new range kernel. Signal Processing, 137, pp.223-234.

[35] Huang, D., Wang, Y., Song, W., Sequeira, J. and Mavromatis, S., 2018, February. Shallow-water image enhancement using relative global histogram stretching based on adaptive parameter acquisition. In International Conference on Multimedia Modeling (pp. 453-465). Springer, Cham.