Biosc.Biotech.Res.Comm. Special Issue Vol 13 No 13 (2020) Pp-165-170

BBRC
Bioscience Biotechnology Research Communications

Center Pixel Based Robust Color Image Steganography for IoT Applications

Shyla. M.K[1], K.B. Shiva Kumar[2] and Rajendra Kumar Das[3]
[1]*Department. of Electronics and Communication, Sri Siddhartha Institute of Technology, Tumakuru, Karnataka, India,*
[2]*Department. of Electronics and Telecommunication Engineering, Sri Siddhartha Institute Of Technology, Tumakuru, Karnataka, India,*
[3]*Principal, DRIEMS, Tangi, Cuuttok, Odisha, India*

ABSTRACT

Image steganography is an emerging security technique to secure Intermet of Things based data. The sensitive data transferred or stored in the cloud storage has to be protected from the fraudulence. Any sensitive data from base station or an IoT device can be securely stored in cloud so that only intended user could access by using image steganography techniques which gives authentication. In this image steganography approach, the cover image is divided in to 3X3 matrices. The center pixels of the blocks are extracted to retain the feature of original cover image. This extracted center pixels are performed Exclusive-OR operation with the payload image. After XOR operation the image is shuffled by bit position and then embedded in to the original cover image. The proposed method is tested for several input images to show the robustness and shuffling is based on bits interchange instead of interchanging rows and columns hence the algorithm is more secure. The proposed approach uses the extracted center pixels as key for embedding instead of Local Binary Pattern encoding which reduces the complexity in computation and hence save the power required for any IoT applications.

KEY WORDS: AUTHENTICATION, CENTER PIXEL BASED, CLOUD STORAGE, IOT DEVICES, ROBUSTNESS.

INTRODUCTION

Many techniques have been implemented to reduce the information disclosure among IoT devices (Arun et al., 2020). Cryptography and steganography are mostly widely used techniques where cryptography uses encryption to get cipher text at the transmitter side and the decryption is used at receiver side to extract message, these process of encryption and decryption may demands more processing and memory (Parameshachari et al., 2020). Since conventional cryptography uses more processing and memory which is a major constraint in IoT devices, light weight cryptographically based algorithms can be used with lesser programming and memory size, again in which system may not be secured. Since input information itself is scrambled in to some other form, eavesdropper can be easily noticed and this becomes major drawback of cryptography. Steganography is the technique used to overcome this drawback where the input message is retained as it is and embedded in some other cover medium such as text, video, audio or an image files.

Real time data transmission from any location is made easy with the growth of internet technology and its usage has spread all over the world and the communication is made more economical. When the Internet is used by public more in nature then the security attacks become the biggest disadvantage and the interesting aspect is the easy accessibility of the same. In order to reduce the malicious attacks, covert communication using steganography is widely used technique and plays a vital role.

ARTICLE INFORMATION

*Corresponding Author: shylamk@ssit.edu.in
Received 7th Oct 2020 Accepted after revision 28th Dec 2020
Print ISSN: 0974-6455 Online ISSN: 2321-4007 CODEN: BBRCBA

Thomson Reuters ISI Web of Science Clarivate Analytics USA and Crossref Indexed Journal

Clarivate Analytics

crossref

NAAS Journal Score 2020 (4.31)

Online Contents Available at: http//www.bbrc.in/
Doi: http://dx.doi.org/10.21786/bbrc/13.13/23

Cloud based IoT applications make use of images with digital contents mainly for user authentication and information hiding. Digital Image steganography can be used to hide digital contents in the images to maintain secrecy of information which is received from an IoT device. Even though the IoT infrastructure is useful to mankind, problems or issues arise during data transfer especially in transferring sensitive images. The sensors collect data from the ground station or environment and transfer them through insure public communication channels. Any hackers can access data and manipulate it resulting in the threat to security.

Digital Image steganography is the method of embedding payload information within a carrier such that the existence of payload data is concealed within it (Jung KH 2016). Basically there are two popular methods of image steganography techniques are there; which are reversible (Hong W, Chen TS, 2011) and Irreversible (Hwang et al., 2006). The carrier image can be extracted properly without any loss of data from the received stego image is called as reversible (Kim K et al., 2009). In some techniques, cover image features are lost during embedding process which is known as irreversible steganography (Lin CC, Tai WL, Chang CC, 2008).

Least significant bits based image staganography (Ker A, 2004). Techniques that are proposed in order to embed payload messages in LSB of carrier using both gray scale and color images (Mielikainen J, 2006). These methods adopt some modification in their embedding process to get the visually less distorted stego image. Least significant bit modified techniques check the cover and payload LS bit; if they are equal then it adds 01 to cover otherwise subtracts 01 from cover. LSBM retains some of original carrier features by retaining the equal intensity levels.

MATERIAL AND METHODS

Since the fact that any image and its pixel values are treated as series of binary values, some of the carrier image pixel strings may be replaced with the payload image pixel strings. Least significant bits of carrier can be considered for this replacement since it will not disturb the visual quality of carrier. In opposite, if any modification on the most significant bits leads to maximum degradation of the carrier and it may be visually more distorted (N. Akhtar et al., 2014),

Carrier image and stego image pixels are synchronized in order to maintain the local relationship with carrier image in the modified version of LSBM. LSB matching revisited (Hempstalk K, 2006) is a modified form of LSBM, but results in low embedding rate in retaining the local relationship between carrier and stego image. The technique proposed was based on pixel pair, where one bit of payload is embedded in to the two adjacent pixels of carrier image and its relationship between pixel pair acts as key for embedding. The approach proposed in (Bai J et al., 2017) is based on pixel intensity edge detection where it determines edge and non-edge pixels of the cover image. Another steganography technique to hide payload data explained in (Luo W et al., 2010) is by making use of cover image edges in order to increase the embedding capacity. Different filters are used to identify edges and the payload data is embedded in these edges.

Cover image is rotated using string of secret keys and then edges are detected in the rotated cover image to hide the payload data and are proposed in non blind steganography for images on least significant bits replacement (Chakraborty S et al., 2017), where payload data is embedded into the fringe area of an image in a compatible manner. Another LSB and pixel value differencing based technique proposed in (Khodaei M, Faez K, 2012) where maximum data can be embedded in the non fringe pixels to increase embedding rate. The technique proposed in (Kodovsky J et al., 2012) is based on classifiers and PVD method in which payload data is adaptively hidden into the chosen block of cover image. Another method (Swain G, 2016) where it combines horizontal and vertical edges.

The method proposed in (Hussain M, et al., 2016) is a combination of LSB and PVD which uses recursive shift in difference value of pixels and MPE method to increase payload capacity. The other PVD based techniques which adopts interpolation properties to embed data (Luo L, et al., 2010) and seven different ways to embed secret bits are proposed in (Pradhan A, et al., 2016). All of these methods results in maximum change in the visibility of the stego image with increase in their embedding capacity (Baluja S, 2017). In order to hide the sensitive images other techniques based on deep learning are introduced in (Meng R, et al., 2018) Sensitive payload images are modified with respect to cover and then trained using classifiers and encoders are used for encoding the cover and payload data.

The techniques based on features of image for data hiding have been proposed (Biswas, et al., 2019). The LBP based steganography where the cover image is transformed to get wavelets and local binary patterns are generated to embed payload data. The transformation used is haar function based and is proposed in (Singhal A, and Bedi P, 2016). The scale invariant feature based transform is used to hide the information (Sahu N, Sur A, 2017). Wavelet transform based on integers, division on block based, local binary pattern based on symmetric canter positions are the different techniques used for embedding the data and explained in (Tuncer T, Kaya M, 2019).

Proposed Method: In the present scenario, image steganography can be used to secure personal and sensitive information such as face of an IoT user. Consider a scenario of a local area network where the image captured from an IP camera which can be considered as IoT device can be sent and saved in cloud storage. Eves dropper, who keep on monitor this network can hack the image and affect the system. The proposed method and the block diagram is shown in figure1. The cover image is preprocessed in which the cover image

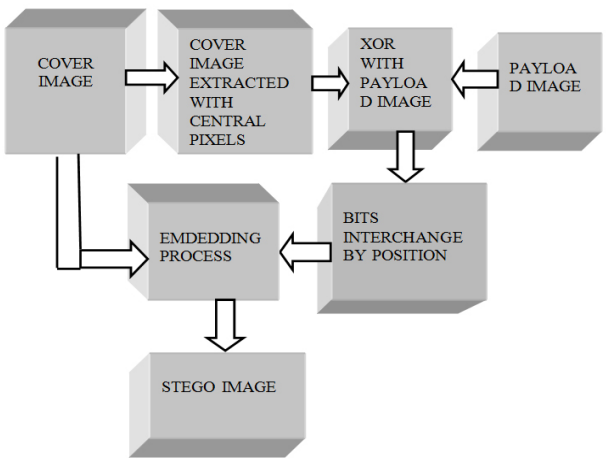
divided in to 3X3 blocks and the center pixel of each block is extracted.

The extracted cover image is XORed with payload image to retain some of the features of carrier image. Further the same center pixels act as key for embedding process. The center pixels are surrounded with 8 pixels and these pixels are used for embedding. Here up to 4 bits of cover image pixels are used for embedding. In the preprocessed method the extracted center pixels are XORed with payload pixels and then shuffled by interchanging bit positions; in this approach 1st and 4th bit positions are interchanged. Then the embedding process is done by block wise synchronized LSB substitution method.

In the embedding process, the last bit with highest weight P7k; l of P (k, l) is placed into the right corner of C(i + 0, j + 1) of C(i, j) as shown in the equation (1). Where P(k) represents the byte obtained after bit interchange, C(i, j) represents the cover image and S (i, j) is the obtained stego image. Similarly, remaining bits of P (k) are embedded into the remaining adjasacent pixels of C(i, j). In order to retain the local neighbourhood relationship with original cover, the stego image pixels are synchronized with extracted center pixels. The resulted stego image is more secure to transmit over internet and can be saved in cloud. Illustration of embedding Process is shown in figure2, where few sample pixels of a cover image are considered for reference.

$$S(i+0, j+1) = \sum_{a=1}^{7} 2^{a} \times c^{a}_{i+0,j+1} + p^{7}_{k,1} \quad \text{.....(1)}$$

Figure 1: Proposed block diagram



The center pixel is extracted and XORed with a sample pixel of payload image and the process of embedding is shown. The recovery of the original payload and its process flow is shown in the figure.3; the block diagram shows that the center pixels are extracted from the stego image. Then the embedded payload bits are extracted and get bits interchanged. XOR operation is performed with center pixels extracted to get original secret image. Extraction process is depicted in figue.4 by considering one sample pixel as an example. An example is explained by considering one pixel of embedded stego image. In the recovery process, the original payload is recovered from the stego image and the process flow is shown in figure.4. The bits after the interchanging in their bit positions with the pixel P(k, l) of the payload are retrieved from the local neighbourhood of each reference pixel S (i, j) of the stego image.

Figure 2: Illustration of embedding process

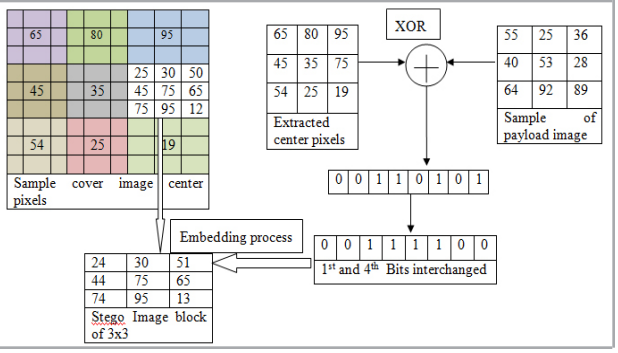


Figure 3: Block diagram of Extraction process

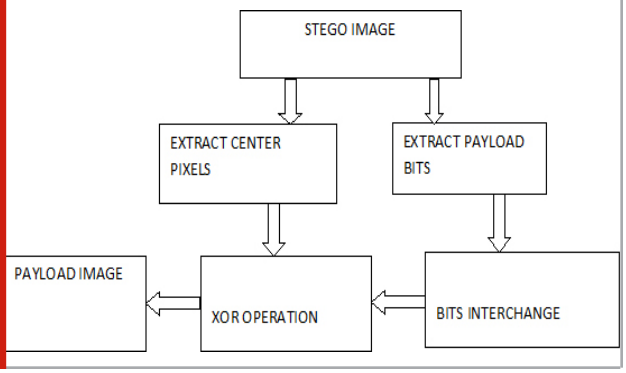
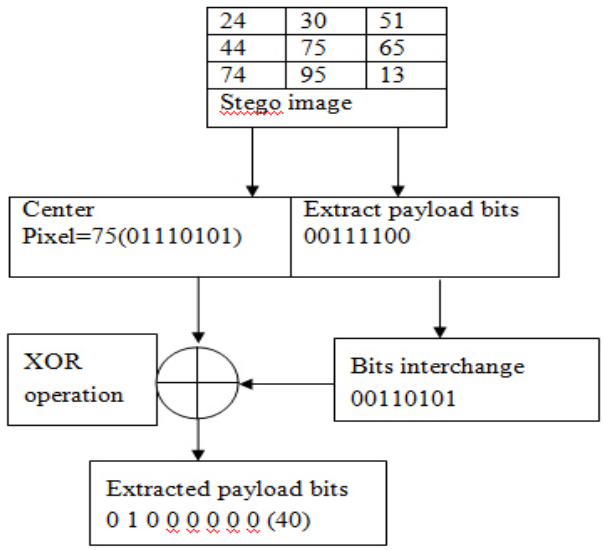


Figure 4: Illustration of extraction process



RESULTS AND DISCUSSION

The proposed method of image steganography reduces the computation complexity of LBP encoding (Soumendu Chakraborty & Anand Singh Jalal, 2020) hence reduces the power consumption and also retaining the local relationship of the cover image pixels with its center pixel to give better visual quality of stego image. An intruder has less suspicion about the existence of data bits around center pixels, because less lsb changes per pixel and out of 8 pixels only three to four pixels are going to change to hide one pixel of a payload image and thus ensures better visual quality. Table 1 gives the comparisons in terms of results for different parameters like Quality index (Q) and PSNR. Figure.5 shows the experimental result for one gray scale image and the corresponding histogram of cover image and stego images respectively. The proposed method is implemented using color images and resulted with good PSNR, different parameters like Quality index or SSIM and mean square errors.

Table 1. Performance analysis in terms of PSNR and Quality index (Q) for gray scale images

Gray Scale image	Soumendu Chakraborty & Anand Singh Jalal, (2020)	Proposed Method	Soumendu Chakraborty & Anand Singh Jalal, (2020)	Proposed Method	Soumendu Chakraborty & Anand Singh Jalal, (2020)	Proposed Method
	PSNR		Embedding Rate (ER)		Quality Index (Q)	
Tiffany	58.25	81.36	3.52	3.55	09995	0.9976
Boat	57.95	80.32	3.47	3.42	0.9987	0.9956

Figure 5: Experimental results of proposed method using gray scale images.

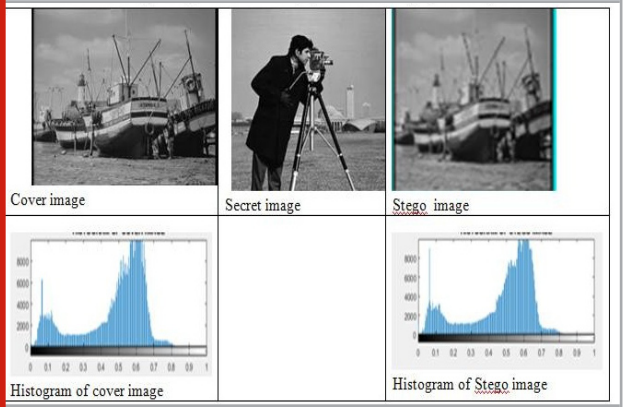
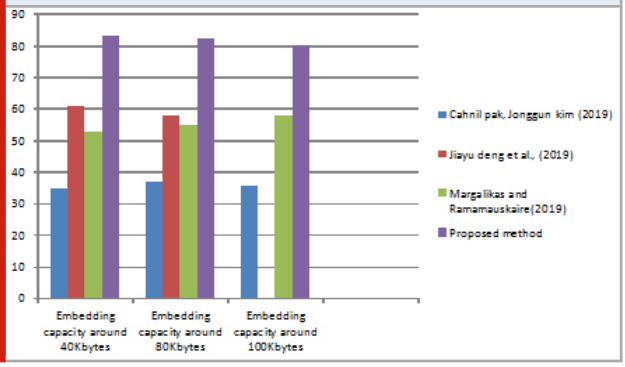
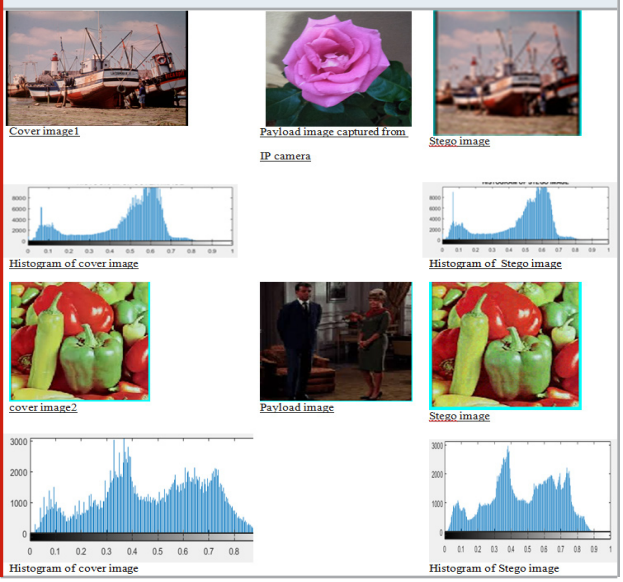


Figure 6: Comparisons of PSNR values using color images between existing and the proposed method.



Entropy calculations are done to estimate the change in bits and the result shows better values and hence the method is more secure. Structural similarity measurement is a quality assessment method done between Stego and cover image and if the value is near to one indicates similarity between the two is more and the result obtained is 0.9998 which is very much near to one hence shows the larger similarity. PSNR values for different embedding capacities between the existing methods like color image steganography using one dimensional chaotic map (Cahnil pak, Jonggun kim, 2019), color image embedding based on cyclic chaos (Jiayu et al., 2019), color palattte in color space (Margalikas and Ramamauskaire, 2019) and proposed method using color images is shown in figure 6.

Figure 7: Experimental Results of the proposed method for color images



Peak signal to noise ratio is measured as a ratio between image and compressed or embedded image as a quality measurement. Higher the PSNR values better the image quality. It is measured by first calculating the mean square error between two images and then consider the ratio between maximum fluctuations of an image and MSE values.

For gray scale images maximum fluctuation can be 8 where as for color images it will be 255. Figure.7 shows the experimental results and histogram comparisons for two images of different sizes and the embedding capacity of 935712 bits which gives the payload or secret bits and MXN is size of the cover image in pixels.

$$EmbeddingRate = \frac{S}{M \times N} bpp \quad (2)$$

Embedding Rate (ER) is used to evaluate the percentage or the amount of payload bits embedded in the cover as shown in equation 2 where S is the total number of payload or secret bits and MXN is size of the cover image in pixels.

CONCLUSION

The proposed method retains the local features of the carrier in the embedded stego image by extracting center pixels of cover and hence the obtained stego image is visually very less distorted. The algorithm is tested for several images taken from the database which gives the better results with respected to various parameters. The work is executed for images captured from IP camera which is considered as an IoT device at the base station. The captured sensitive image can be embedded in to the common images and can be sent over internet to store in the cloud for further usage. The proposed method is implemented in gray scale and the results are compared with the existing methods and also executed for color images and it is resulted with good PSNR for different embedding capacities. Further the proposed method could be used to embed more than one type of inputs in its RGB layers separately and hence can be effectively used for IoT applications.

REFERENCES

Arun, M., Baraneetharan, E., Kanchana, A., & Prabu, S. (2020). Detection and monitoring of the asymptotic COVID-19 patients using IoT devices and sensors. International Journal of Pervasive Computing and Communications.

Bai J, Chang CC, Nguyen TS, Zhu C, Liu Y (2017) A high payload steganographic algorithm based on edge detection. Displays 46:42–51

Baluja S (2017) Hiding images in plain sight: deep steganography. Advances in Neural Information Processing Systems.

Biswas, R., Mukherjee, I., & Bandyopadhyay,

S. K. (2019). Image feature based high capacity steganographic algorithm. Multimedia Tools and Applications, 1-18.

Chakraborty S, Jalal AS, Bhatnagar C (2017) LSB based non blind predictive edge adaptive image steganography. Multimed Tools Appl 76(6):7973–7987

Cahnil pak, Jonggun kim (2019) A Novel color image LSB steganography using improved 1D Chaotic map. Multimedia tools and applications,2019. https;doi.org/10.1007/s11042-019-08103-0.

Hong W, Chen TS (2011) Reversible data embedding for high quality images using interpolation and reference pixel distribution mechanism. J Vis Common Image Represent 22:131–140

Hempstalk K (2006) Hiding behind corners: using edges in images for better steganography. Computing Women's Congress Proceedings, Hamilton, New Zealand.

Hussain M, Wahab AWA, Javed N, Jung KH (2016) Recursive information hiding scheme through LSB, PVD shift, and MPE. IETE Tech Rev:1–11.

Hwang J, Kim JW, Choi JU (2006) A reversible watermarking based on histogram shifting. Lecture Notes Computer Science 4283:348–361

Jiayu deng, Mingwei tang, Yantig wang, Zhen wang (2019) LSB Color image embedding steganography based on cyclic chaos. 2019 IEEE 5th international conference on computer and communications Pg.No.1798-1802.

Jung KH (2016) A survey of reversible data hiding methods in dual images, IETE Tech Rev 33(4):441–452

Khodaei M, Faez K (2012) New adaptive steganographic method using least-significant- bit substitution and pixel-value differencing. IET Image Process 6(6):677–686

Ker A (2004) Improved detection of LSB steganography in grayscale images, information hiding workshop, Toronto, Canada, May 23-25, vol. Springer LNCS 3200:97–115

Kim K, Lee M, Lee H, Lee H (2009) Reversible data hiding exploiting spatial correlation between subsample images. Pattern Recogn 42(11):3083–3096

Kodovsky J, Fridrich J, Holub V (2012) Ensemble classifiers for steganalysis of digital media. IEEE Transactions on Information Forensics and Security 7(2):432–444

Lin CC, Tai WL, Chang CC (2008) Multi level reversible data hiding based on histogram modification of difference images. Pattern Recogn 41(12):3582–3591

Luo L, Chen Z, Chen M, Zeng X, Xiong Z (2010) Reversible image watermarking using interpolation technique. IEEE Trans Inf Forensics Secur 5(1):187–193

Luo W, Huang F, Huang J (2010) Edge adaptive image steganography based on LSB matching revisited. IEEE

Trans Inf Forensics Secur 5(2):201–214

Margalikas and Ramamauskaire(2019). Image steganography based on color palette transformation in color space. EURASIP Journal on Image and video Processing (2019)

Meng R, Rice SG, Wang J, Sun X (2018) A fusion steganographic algorithm based on faster R-CNN. Computers, Materials & Continua 55(1):1–16

Mielikainen J (2006) LSB matching revisited. IEEE Signal Process Lett 13(5):285–287

N. Akhtar, S. Khan, and P. Johri (2014), "An improved inverted LSB image steganography," in Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014 International Conference on, 2014, pp. 749 -755.

Parameshachari, B. D., Panduranga, H. T., & liberata Ullo, S. (2020, September). Analysis and Computation of Encryption Technique to Enhance Security of Medical Images. In IOP Conference Series: Materials Science and Engineering (Vol. 925, No. 1, p. 012028). IOP Publishing.

Pradhan A, Sekhar K R, Swain G (2016) Digital image steganography based on seven way pixel value differencing. Indian Journal of Science & Technology 9(37):1–11. https://doi.org/10.17485/ijst/2016/v9i37/88557

Swain G (2016) Adaptive pixel value differencing steganography using both vertical and horizontal edges. Multimedia Tools and Application 75(21):13541–13556

Singhal A, and Bedi P (2016) Local binary pattern operator based steganography in wavelet domain. 2016, International Conference on Advances in Computing, Communications and Informatics (ICACCI).

Sahu N, Sur A (2017) SIFT based video watermarking resistant to temporal scaling. J Vis Commun Image Represent 45:77–86.

Soumendu Chakraborty & Anand Singh Jalal (2020) A novel local binary pattern based blind feature image steganography, Multimedia Tools and Applications, Mar 2020

Tuncer T, Kaya M (2019) A novel image watermarking method based on center symmetric local binary pattern with minimum distortion. Optik 185:972–984.