Advances in Computer Science and Information Technology (ACSIT)
p-ISSN: 2393-9907; e-ISSN: 2393-9915; Volume 4, Issue 3; April-June, 2017, pp. 166-170

http://www.krishisanskriti.org/Publication.html

Steganography Based Edge Detection using Fuzzy Logic Technique

Juhi[1] and Rajesh Mishra[2]

[1]*ICT Department, Gautam Buddha University, Greater Noida*
[2]*Gautam Buddha University, Greater Noida*

Abstract—*In the spatial domain, least significant bit (LSB) technique is one of the generally used steganographic algorithms. The image content itself did not precisely resolve in most extent schemes. Therefore the smooth areas in the cover image will obligatory be corrupted after hiding even at a low embedding rate, so it leads to indigent visual quality and poor security. Several steganography methods using edge detection have been proposed recent years. For the sake of storing edge information in the cover image, there schemes employ certain pixels, emerging in significant embedding distortion and low payload. In this paper, LSB substitution and edge detection based steganographic approach is proposed. To evade the removal of human visual system(HVS) when more secret bits are enclosed into pixel, we arrange the cover pixels into edge areas and non-edge area. More secret could be carried by the pixel that belong to the edge pixel. The same edge information is obtained in the extraction phase. So without confusion secret data can be extracted.*

Keywords: *Least-significant-bit (LSB) substitution, Edge detection, Human visual system, Fuzzy logic, High payload, Digital image processing*

1. INTRODUCTION

Internet makes the present day society digitalized and facilitates us to readily share immense data by pervasive channels. For exchanging information, downloading, uploading and manipulating internet makes it ease. In day-to-day life, thousands information are generally transferred. If the security of network multimedia has not well secured, it affirms a probable problem that may result in disclosure of our privacy to the public. So a secure communication is a crucial demand if we want to send the confidential data via internet. Generally, for a authentic and secure transmission cryptography has been used. Nevertheless, the data encryption which is senseless message may in fact be called doubt from illegitimate attackers. Presently, to distract any particularly regard from attackers, steganography is devised to conquer this drawback by inconspicuous inserting confidential into a cover media. In this study, we target on steganography based on digital images. To protect the privacy of information from vigilance and intellectual property from imitation, these steganography mechanisms are examined. These include following methods fingerprinting, digital signature, covert channel and spread spectrum communication. There exists a well known visual requirements model called a magic triangle, in information hiding which was proposed in 2001 by Johnson. Magic triangle is the combination of capacity, imperceptibility and robustness. Capacity is the first requirements, called as embedding payload. The total no of secret bits that can hide into cover image is termed as capacity. The cover image will carry the more secret bits means higher capacity is achieved. The image quality is measured by the imperceptibility, calculating the peak-signal-to-noise (PSNR) is the second requirement.Embedding manipulation leads to the introduction of distortion and it should be as limited enough to assurance that it can not be determined by human visual system(HVS) because of visible artifacts.

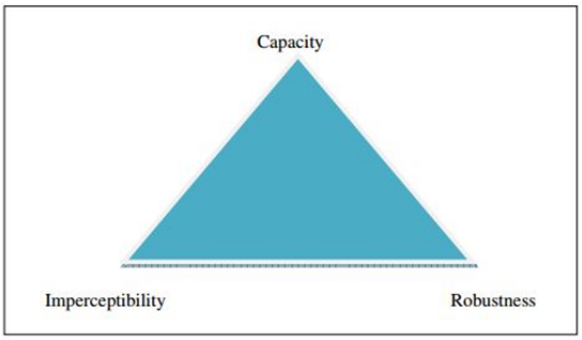

Fig. 1.1: Steganography magic triangle model

These three requirements shows the interrelationship. The triangle at a relatively high level keeps the quality of stego image under a certain degree of attacks. In the field of information hiding it becomes an interesting issue that how to balance these requirements.

Least significant bit substitution is the classical steganographic mechanism in terms of high payload and low computational complexity which provide great performance. To indicate the secret message the value of the lowest bits of pixels in the host image is utilized which means secret bit modified the LSBs of the pixel of the cover image. By

reading the lowest bits of pixels in the stego image, on the receiver end, the recipient extracts the confidential message. Even if the high insertion capacity is achieved by the LSB substitution mechanism, in a digital image, the amount of secret data which can be embedded usually varies widely from region to region. All pixels can not carry the same degree of changes. Therefore, several scholars have been proposed some discreet LSB-based methods to reduce this shortcoming. In 2000, For optimal LSB substitution scheme Wang at el. Proposed an exhaustive search. Then in 2003, Chang at el. proposed a utilizing dynamic programming strategy for data hiding, i.e an optimal model. Here they get the stego image with finite capacity and discontent quality. Wu et al. exploited the difference value in two consecutive pixels and combined it with the LSB substitution method. Jana at el. exploited new reversible data hiding scheme for embedding n-1 secret bits based on high relation of two consecutive pixels. The shared secret key bit stream is used to distribute the stego pixel pair into dual images to enhance the security of embedding data. It provides limited image quality and embedding data. Smooth area frequently change irrespective of edge area does.

2. PROPOSED METHOD

Related Work

2.1 Edge Detectors

Edge finder assumes a moderately essential part in the field of computer vision for recognizable description and grouping of objects, and is likewise a standout amongst the most normally utilized operations in image processing field. Edge can be described as a form at which a noteworthy uniqueness happens in some physical aspect of a picture, such as in grey levels. Basically, edge discovery is received to demonstrate the unexpected changes in the intensity of a picture and recognize the current pixel a non-edge pixel or an edge pixel. An a lot of traditional edge finders have developed through the literature, i.e., Sobel, Robert, Laplacian, Prewitt, Fuzzy, and Canny edge detectors. Among them fuzzy logic edge detector (FLED) are utilized prevalently in the scholarly community and industry. FLED achieves flexibility and robustness under different attacks.

2.1.2 FLED

The process of transmitting a given input value to an output using fuzzy logic is called the fuzzy inference. Here four inputs and one output is given for the fuzzy inference system.

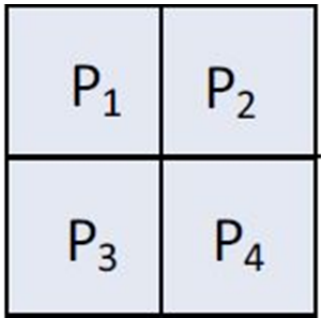

Fig. 2.1: 2*2 pixels window

For the four pixel values of the window mask four inputs are used. Keeping in mind the end goal to stay away from the intricacy, checking mask of 2×2 pixels window is utilized. A fuzzy surmising based framework has been outlined under MATLAB stage to identify the edge. A run base comprising of 16 principles has been created to distinguish the pixel under thought in a 2×2 window as White, Edge or Black.

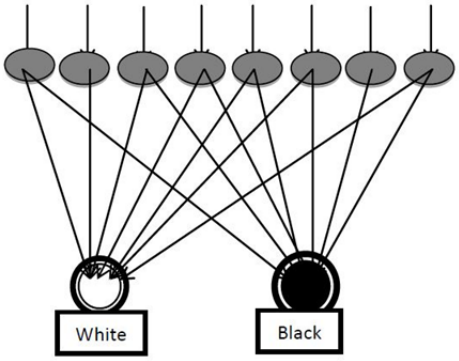

Fig. 2.2: Fuzzy Model

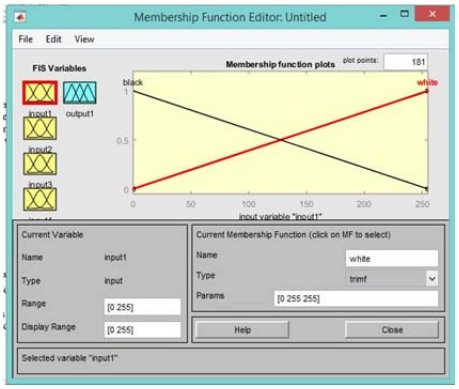

Fig. 2.3: Membership functions of the fuzzy sets associated to the input

The fuzzification of information is accomplished by two fundamental trapezoidal enrollment capacities called Black and White. An assessment of these two capacities, all the picture pixels (fresh set) is characterized into Black or White fuzzy sets. The pixels are fuzzified in the fuzzy induction framework, and rule base of FIS, have been characterized to apply suggestion on the sources of info. The inference rules rely on upon the weights of neighbors i.e. P1, P2… Pn and itself, i.e. the weights are level of Black or level of White. These weights are joined utilizing AND administrator as characterized in the rule base. The output of applying suggestion is again fuzzy.

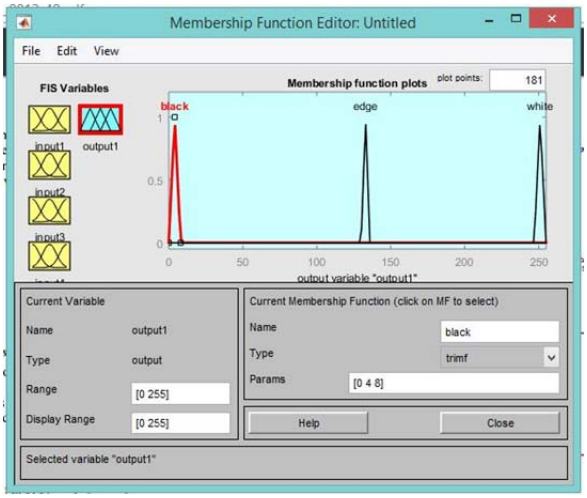

Fig. 2.4: Membership functions of the fuzzy Sets associated to the output

In FLED, a pixel is set apart as an edge if the intensity variety between the adjoining pixels is sharp. The outlined approach has four input and one output. As indicated by the four information sources, sixteen rules are resolved as appeared in Table 1, where B, W and E, mean the pixel under thought as black, white, and edge, individually.

Table1: Fuzzy set parameter

Fuzzy Input				Fuzzy Output
P1	P2	P3	P4	$P4_{out}$
B	B	B	B	B
B	B	B	W	E
B	B	W	B	E
B	B	W	W	E
B	W	B	B	E
B	W	B	W	E
B	W	W	B	E
B	W	W	W	W
W	B	B	B	E
W	B	B	W	E
W	B	W	B	E
W	B	W	W	E
W	W	W	B	E
W	W	B	W	E
W	W	W	B	E
W	W	W	W	W

Image steganography using LSB substitution technique

The least signicant bit (the eighth bit) of a few or the greater part of the bytes inside a picture is changed to a bit of the mystery message. Digital pictures are basically of two sorts (i) 24 bit pictures and (ii) 8 bit pictures. In 24 bit pictures we can embed three bits of data in every pixel, one in each LSB position of the three eight bit values. Expanding or diminishing the incentive by changing the LSB does not change the presence of the picture; much so the resultant stego picture looks practically same as the cover picture. In 8 bit pictures, one piece of data can be covered up.

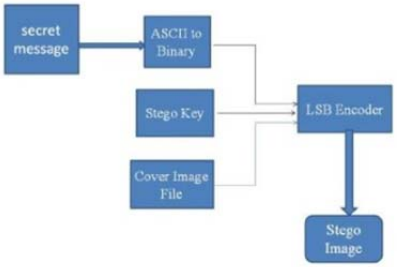

Fig. 3a: LSB insertion mechanism

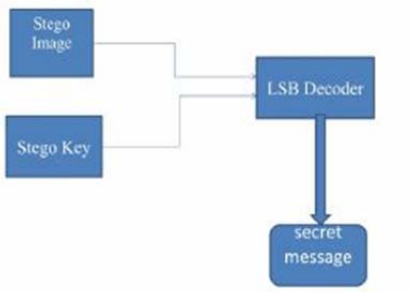

Fig. 3b: LSB extraction mechanism

RESULTS AND DISCUSSION

Table 2: PSNR of Pseudo-Random Encoding

Sl no	Cover Image	Secret Message	Stego Image	MSE	PSNR
1	Gray image	Text message	Gray-Image	0.0112	62.6065
2	RBG image	Text message	RGB image	0.0011	66.6535
3	RBG image	Image	Images	0.0711	56.5346
4	Edge Image	Text message	Images	2.321	73.432
5	Edge Image	Image	Images	3.982	75.681

Table 3: PSNR of Least Significant Bits Encoding

Sl no	Cover Image	Secret Message	Stego Image	MSE	PSNR
1	Gray image	Text message	Gray-Image	0.0102	62.5065
2	RBG image	Text message	RGB image	0.0211	66.6325
3	RBG image	Image	Images	0.0721	55.5346
4	Edge Image	Text message	Images	2.221	73.132
5	Edge Image	Image	Images	3.782	75.481

Image steganography using edge detection mechanism

This section proposes another LSB steganography show in view of edge detection mechanism. The procedure of embedding and extracting are two vital modules of this scheme like some other steganographic framework.

Fig4a Original Image

Fig. 4b Edge detection using fuzzy

Fig. 4c Original image

Fig. 4d Edge detection using sobel

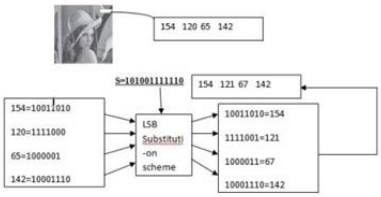

Fig. 5a Example of the proposed embedding phase.

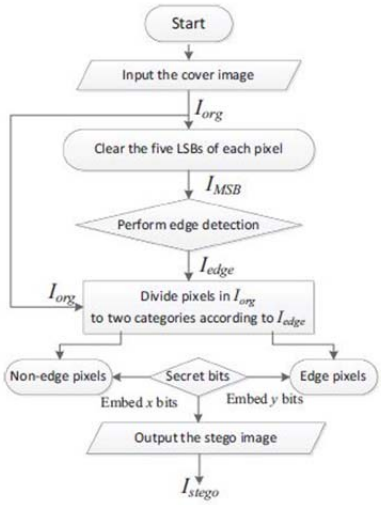

Fig. 5b The flowchart of the proposed embedding phase.

Embedding phase

The flowchart of the whole inserting methodology is shown in Fig. 6. On the premise of the got edge picture Iedge produced from Imsb, we group the pixels of the first cover picture Iorg into two classes which are non-edge pixels and edge pixels, separately. Like Chen et al's. plan, we use two parameters x and y, where x implies the quantity of mystery bits to be installed into non-edge pixels and correspondingly y implies the quantity of mystery bits to be installed into edge pixels. For these two classifications, pixels are implanted by the k-LSB substitution, where the esteem k measures up to either x or y which is chosen by the edge data. At last, we acquire the stego picture by inserting the estimations of x and y into four last pixels of the picture. For security reason, two parameters, x and y, ought to be scrambled with the mystery key K which is shared between the sender and the collector ahead of time.

2.3.2 Extraction Phase

In the extraction stage, the receiver initially remove the two parameters x and y from the last four pixels of the picture. Likewise, the edge data is resolved the same as in the installing stage. Along these lines, the mystery information will be removed precisely.

2.4. Experimental results

The implanting limit (likewise called payload) is measured by the most extreme number of installing bits per pixel (bpp). It is characterized as takes after:

Bpp=Maximal embedding bits /H*W

where H and W are the height and width of the original cover image, respectively.

The nature of the stego picture is measured by the accompanying two perspectives.

The PSNR is defined as:

$$PSNR = 10 \cdot \log_{10}\left(\frac{255^2}{MSE}\right)(\text{dB}),$$

where the MSE is the mean square error between the pixels in original image and in stego image. For a cover image with height H and width W, MSE is defined as:

$$MSE = \sum_{i=1}^{n}\sum_{j=1}^{w}(p_{ij} - p'_{ij})^2/(H \times W),$$

where pij and p'ij refer to pixel values of the original and the stego images, respectively. Obviously, a higher PSNR means a better quality that the stego image is very close to the original image.

Table 4: Experimental results of the proposed scheme using various values of x and y on 'Lena' image size of 128 *128.

		Sobel		Fuzzy	
x	y	psnr	payload	psnr	payload
1	2	51.423	1.184	48.001	1.893
1	3	47.852	1.096	41.214	2.673
1	4	43.011	1.214	35.593	3.418
1	5	42.121	1.172	26.250	4.271
2	3	45.976	1.986	40.165	2.893
2	4	42.239	2.196	32.544	3.681
2	5	40.271	2.014	27.342	4.481
3	4	38.341	2.212	32.122	3.921
3	5	37.279	3.086	27.301	4.568
4	5	32.094	4.241	28.194	4.983

3. CONCLUSIONS

In this paper, we proposed a novel steganographic conspire by utilizing the edge identifier which accomplishes a somewhat high payload without presenting a discernible twisting. The best approach to produce the edge picture is not the same as traditional operations. In our strategy, the edge picture is created by clearing the last 5 LSBs operation to the first picture called MSB picture. It contributes to making bigger inserting space than the current plans since the pixels in the picture portion relinquish going about as lists to store edge data. Our implanting standard can simply function admirably under distinctive edge recognition components, i.e Sobel, and Fuzzy identification components. Exploratory outcomes affirm the predominance of our way to deal with regarding higher payload and better picture quality.

REFERENCES

[1] Y.Y. Tsai, J.T. Chen, C.S. Chan, Exploring LSB substitution and pixel-value differencing for block-based adaptive data hiding, Int. J. Netw. Secur. 16 (2014) 363–368

[2] E.K. Kaur, E.V. Mutenja, E.I.S. Gill, Fuzzy logic based image edge detection algorithm in MATLAB, Int. J. Comput. Appl. 1 (2010) 55–58.

[3] C.K. Chan, L.M. Cheng, Hiding data in images by simple LSB substitution, Pattern Recognit. 27 (2004) 469–474.

[4] Y.K. Lee, L.H. Chen, High capacity image steganography model, Proc. IEE Vision Image Signal Process. 147 (2000) 288–294.

[5] H.C. Wu, N.I. Wu, C.S. Tsai, M.S. Hwang, Image steganographic scheme based on pixel-value differencing and LSB substitution methods, Proc. IEE Vision Images Signal Process. 152 (2005) 611–615.

[6] T.S. Nguyen, C.C. Chang, N.T. Huynh, A novel reversible data hiding scheme based on difference-histogram modification and optimal EMD algorithm, J. Vis. Commun. Image Represent. 33 (2015) 389–397.

[7] B. Jana, D. Giri, S.K. Mondal, Dual-image based reversible data hiding scheme using pixel value difference expansion, Int. J. Netw. Secur. 18 (2016) 633–643.

[8] R.M. Davis, The data encryption standard in perspective, IEEE Trans. Commun. 16 (1978) 5–9

[9] D.W.N. Bender, M. Gruhl, A. Lu, Techniques for data hiding, J. IBM Syst. 25(1996) 313–316..