Computerized Steganographic Technique using Fuzzy Logic

Dr. Abdulrahman Abdullah Alghamdi
College of Computing and IT,
Shaqra University, Kingdom of Saudi Arabia

***Abstract*—Steganography is the method of providing Computer security in which hiding the required information is done by inserting messages within other messages, which is a string of characters containing the useful information, in a carrier image. Using this technique, the required information from the secret image is embedded into individual rows as well as columns present in the pixels of carrier image. In this paper, a novel fuzzy logic based technique is proposed to hide the secret message in individual rows and in individual columns of pixels of the carrier image and to extract the hidden message in the same carrier image. The fuzzification process transforms the image in to various bitplanes. Pixel number and Correlation Value is computed in the original image for hiding the secret information in to the original image. The pixel number and Correlation value is also used as the key for retrieving the embedded image from the receiver side. Pixel merging is done in the sender side by assigning a steganographic value of white and black pixels in original image based on the fuzzy rules by comparing the pixels present in the original and secret images. The information which is hided can be retrieved by using the same fuzzy rules. Experimental results show that the proposed method can hide and retrieve the secret and important messages in an image more effectively and accurately.**

***Keywords*—Computer security; fuzzy logic; carrier image; secret image; steganography; fuzzification; peak signal to noise ratio**

I. Introduction

The method of hiding an information on a medium as image as is called as Steganography. Steganographic technique is done for the past decades with various enhancements in medium and in the secret images for providing the Computer Security. Information hidden in photographs or an image is more common recently [2], [3], [4]. In this case, the medium of information hiding is an image. An image can be defined as a function of two dimension coordinates f(x, y), where x and y represents the spatial co-ordinates, and f is called as its intensity [1]. In this method an image is considered to be a matrix of two dimension where each point represents its pixel which is the rows and columns. It also has a medium level of brightness. The increased use of multimedia data tends to do fast and convenient exchange of digital information throughout the Internet. With the simplicity of editing and reproduction of the content, the protection of possession for materials of digital audio, video and image video become an important topic of research. In this proposed method, a text which is present in an image is embedded into a gray image. This process can be done by using the fuzzy rule-based region merging. The embedded text can be retrieved easily only by the receiver who knows the defuzzification process. The main importance of this proposed methodology is that it can be used easily by any end user. This methodology solely concentrates on steganography based on an image which is most widely used because of its capacity of carrying hidden data is higher and hence it is very difficult to find a steganographic data from a normal digital image.

The salient features of the proposed Steganographic technique are:

1) It is a completely automatic and an unsupervised method.

2) No assumption is made prior about the type and contents of images which is given as input.

3) This method has a novel information hiding process which is based on fuzzy logic for merging pixels of the carrier image and the secret information present in another image.

4) This method is robust in information hiding since this method incorporates of Fuzzy Logic with region merging.

II. Literature Survey

Many techniques of steganography were proposed by recent researchers [5]-[6], [8]-[10], [11]-[15], [18]. In this paper, various steganography techniques which are based on fuzzy based techniques have only been discussed. Khursheed and Mir in [16], [17] applied the methodologies based on fuzzy logic for hiding information in another data. In their method, they tried to embed the information in a domain based on fuzzy logic. The advantages are lower computationally expense when it is compared to existing domain transformation methods. Their method provides embedding versatility and safety from common cover attacks, as well as appropriate imperceptibility and payload capacity. However, the secret data is sensitive in nature and it is easy to be destroyed by making a small change in the overall cover and by changing without any particular visibility.

Toony et al. [19] proposed a new image hiding method. In their method, a secret information as image is hidden by using a fuzzy based coding and decoding technique. A fuzzy coder compresses each and every block which is there in the form of secret information into a smaller block and utilizes model-based steganography for hiding the entire message towards a carrier image. This creates minimum distortion in the entire image which results in a quality stego image. Main advantage of their proposed methodology is it yields a higher rate in

embedding data and enhancement in the overall security. Hussain et al. [20] designed a methodology based on the combination of a hybrid fuzzy c-means algorithm and support vector machines model for implementing steganography in images. Their proposed model creates the capability of hiding the secret messages which is convertible to visual system of human. This approach has an advantage of clustering feature using Fuzzy C Means Clustering and a classification technique based on support vector machines.

Goodarzi et al. [21] developed a new scheme for steganography based on the Least Significant Bit method for utilizing the hybrid-based edge detector method. Their method uses the edge detection methodology such as canny and edge detection algorithms based on fuzzy logic. This proposed methodology overcomes the Fridrich's based methods, and steganalysis based systems based on the methodology of statistical based analysis. It also generates high quality stego images. Each and every steganography-based method has its own disadvantages. Petitcolas et al. [6] concludes the various disadvantages of various often used steganography systems. Finding and deletion or modification of secret data in a medium is called as steago attacks. These attacks can be described in many forms which are based on various techniques of information hiding. Craver et al. in [7] elaborates three types of steago attacks namely attacks in robustness, attacks in presentation, and attacks in interpretation.

From the works found in the literature, it has been observed that most of the existing works used. Thresholding based algorithm, Fuzzy C means algorithm, neural networks based algorithms and operators for Background removal. However, in case of medical applications, the accuracy provided by various phases of segmentation is not sufficient to make effective decisions. Therefore, it is necessary to propose a new and efficient technique to enhance the accuracy of segmentation.

This paper is organised as follows: Section 3 presents the methodology of the proposed steganographic technique, explaining in detail the use of techniques, such as Fuzzification, Pixel number and Correlation value calculation, Pixel merging based on Fuzzy rules, Retrieving message from stego-image. In Section 4, the complete results obtained for the proposed methodology is presented. Finally, Section 5 presents the conclusions and future enhancements about this work.

III. PROPOSED METHODOLOGY

In this paper, a fuzzy logic based pixel merging method has been proposed for hiding the secret information which is present in an image in to an original image more clearly. This combination of helps to make effective steganographic process regardless of the type of information even the secret information is more or less since it is based on black and white pixels. The proposed methodology is a collection of processing bitplanes of an image and fuzzy logic applied to each pixel present in the original and secret image. Overall architecture of the proposed methodology is shown in Fig. 1.

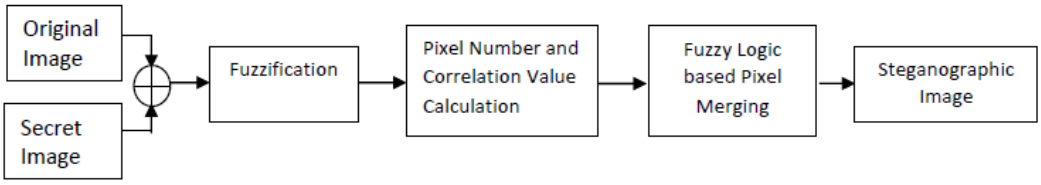

Fig. 1. Proposed steganography method.

A. Generating the Steganographic Image

This proposed method consists of the following steps:

1) The grey scale original and the secret images are considered to be the Input images.

2) The algorithm counts the number of black and white pixels present in both the original and secret images.

3) Since the input images are grey, it is separated into 4 monochrome images in order to obtain the bit values from each bitplanes.

4) The 2 bits which represents the background picture are called as "lower nibble" and the remaining 2 bits which represents the foreground picture called as "upper nibble".

5) Pixel merging is done in the sender side by assigning a steganographic value of white and black pixels to the original image which is based on the rules of fuzzy logic by comparing the pixels present in the original and secret images. It also calculates the pixel number in original image at which the pixel from secret image is merged.

6) A textural property called as Correlation is also calculated for the original pixel. This value is used as the key for receiving the image which is encrypted from the receiver side.

7) Obtained pixels are the steganographic image.

8) Defuzzification is performed by reversing the pixel merging process in the receiver side in order to get the secret information from the carrier image.

B. Fuzzification

The process of changing the values from one crisp sets in to another fuzzy set member for the process of qualitative representation is called as fuzzification. In many Fuzzy segmentation methods such as Fuzzy based clustering, Fuzzy C-means and Fuzzy based inference, intensity transformation of values towards a range of different numerals is done in the initial stage. In this work, the transformation (fuzzification) process as shown in Fig. 2 is equivalent to the formation of 4 bitplanes which is shown in Fig. 3(a)-(h). The input is a monochrome in nature, the entire image contains various pixels of black and white. By observing each bitplane, the gradient of the original image is calculated, and a decision is made whether information hiding is required at such gradients.

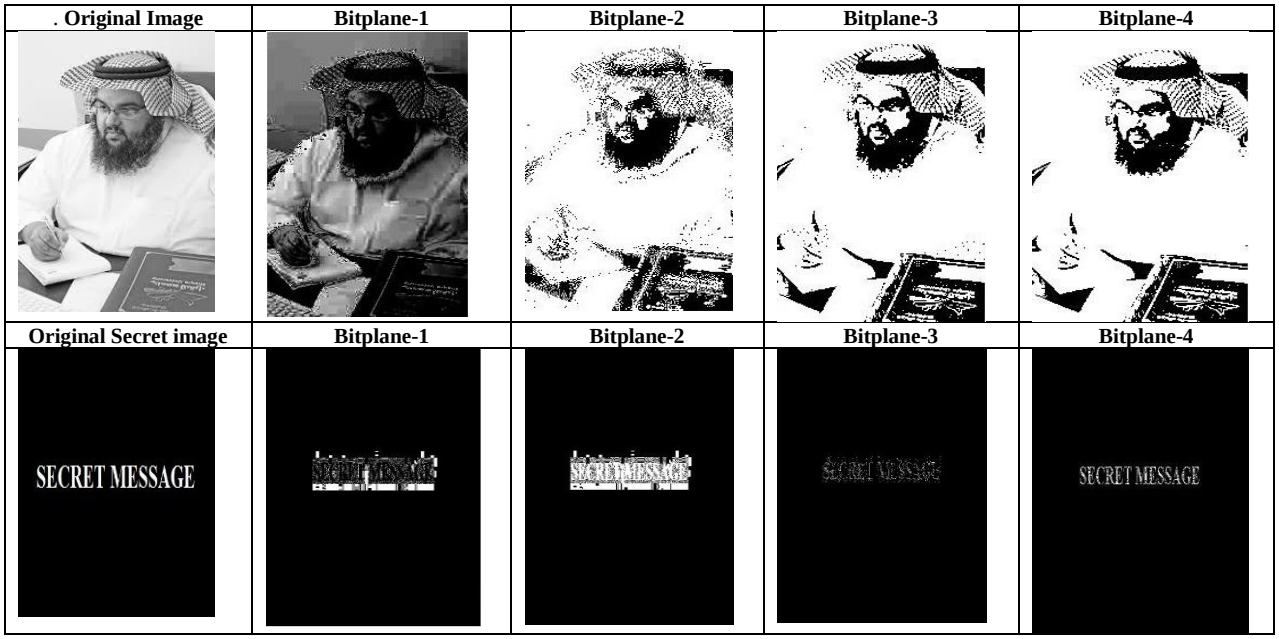

Fig. 2. Results of fuzzification: a) Original image and Secret image, b) Bitplane-1, c) Bitplane-2, d) Bitplane-2, e) Bitplane-4.

C. Pixel Number and Correlation Value Calculation

Pixel number is calculated to identify the place in original image at which the pixel from secret image is merged. It can be used at the point of Retrieving message from stego-image at the receiver side. Calculation of Correlation value is performed as an additional security measure. Correlation value is calculated for the pixels present in the original image and it is merged along with the pixel contains the information from secret image. The formula for calculating the correlation of a pixel is as follows:

$$Correlation = \sum_{ij} \frac{(i-\mu j)(j-\mu j)P(i,j)}{\sigma_i \sigma_j} \quad (1)$$

An intruder who is wishing to detect or modify the hidden data can't predict or calculate the correlation value of the pixel where the data maybe hidden. This ensures that the data cannot be deciphered without the knowledge of both sender or receiver.

D. Pixel Merging Based on Fuzzy Rules

Pixel merging is the process of merging two or more pixels with each other. In this work, the pixel merging is done based on the defined fuzzy rules shown in Table I. Four rules are written for this process. This process compares the pixels of original and secret images and hides the secret image in the original image based on the below rules. Rule 1 compares the first pixel of original image with the first pixel of secret image.

Fuzzy Rule 1: If the pixel in Original image (O) is Black (b) and the pixel in Secret image (S) is White (w) then, go to the next pixel in original image.

Fuzzy Rule 2: If the pixel in Original image is white and the pixel in Secret image is black then, Calculate the pixel number and Correlation value of the entire pixel of the original image. Then, merge the pixel of secret image with original image. After merging, go to next pixel in both images.

Fuzzy Rule 3: If the pixel in Original image is white and the pixel in Secret image is black, then go to the next pixel in secret image.

Fuzzy Rule 4: If the pixel in Original image is Black and the pixel in Secret image is black, then go to the next pixel in both original and secret image.

TABLE I. FUZZY RULES

Fuzzy Rule 1	IF $p_b(O) = p_w(S)$ then Go to the next pixel in original image ENDIF
Fuzzy Rule 2	IF $p_w(O) = p_w(O)$ Then Calculate pixel number and Correlation value. Merge the secret image pixel in original image pixel. Go to next pixel in both images. ENDIF
Fuzzy Rule 3	IF $p_w(O) = p_b(O)$ then Go to the next pixel in secret image ENDIF
Fuzzy Rule 4	IF $p_b(O) = p_b(O)$ then Go to the next pixel in both original and secret image ENDIF

E. Retrieving Message from Stego-image

Pixel number of original along with its correlation value is given as key towards the receiver. The receiver can extract the hidden information from original image by identifying the correct pixel and by subtracting the correlation value from it in order to obtain the original pixel from it. Since the pixel number along with correlation value is considered as a key for extracting the hidden information, the proposed methodology can be taken as more secured when compared to other existing steganographic methods.

IV. Results and Discussion

The proposed methodology is implemented using MATLAB and the resulting image was obtained by giving the input image along with the carrier image. From the result obtained, it can be observed that both the carrier and the output stego-image were indistinguishable visually. The carrier and the secret images are shown in Fig. 3. The efficiency of the proposed method is determined from the Peak Signal to Noise Ratio (PSNR) and the Mean Square Error (MSE) value. The MSE and the PSNR are the two error metrics used for comparing quality of an image. These ratios are often used as a quality measurement between the original and processed image. In general, the higher is the PSNR, the better is the quality of the processed image. MSE is the cumulative squared error which lies between the processed and the original image, moreover PSNR is the measure of peak error. When the MSE value is low, then the error is also Low. These parameters are defined as follows:

$$PSNR = 10\ log_{10}(R^2/MSE\ ) \quad (2)$$

Where, M and N are the number of rows and columns in the input images, respectively. Then the algorithm calculates the PSNR value using the below equation:

$$MSE = \frac{\sum_{M,N}[I_1(m,n) - I_2(m,n)]^2}{M*N} \quad (3)$$

Where, R is the maximum fluctuation in the input image data type.

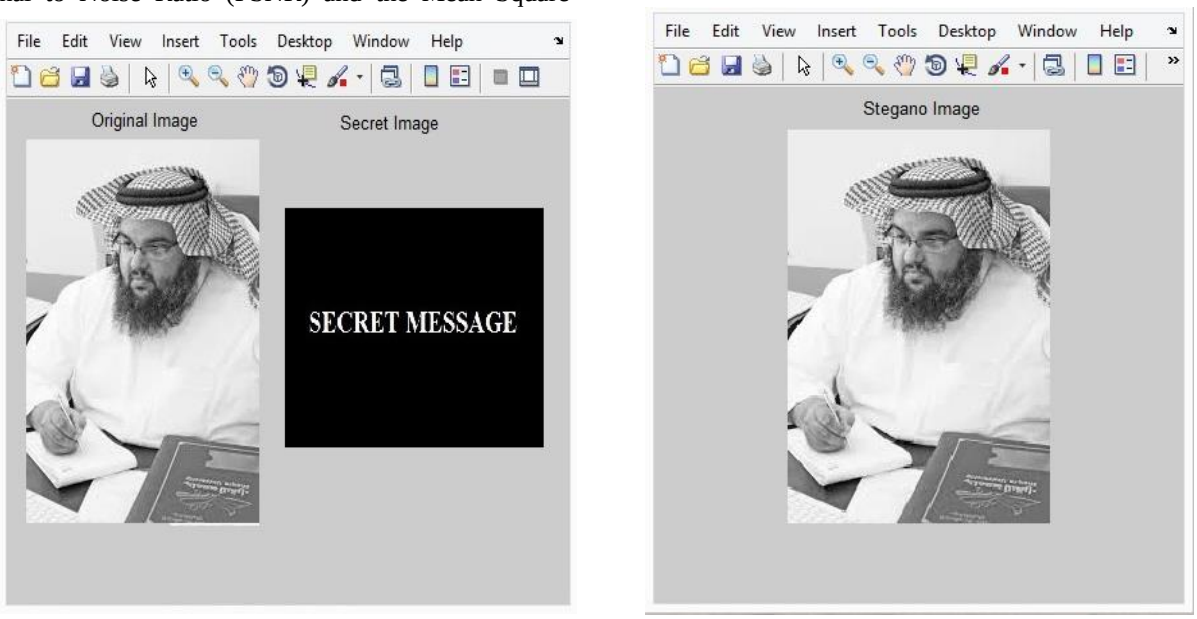

Fig. 3. Results of the original and Steago image.

Table II presents the accuracy estimation based on PSNR and MSE values for some of the sample information as secret image and one original image on which the proposed methodology was implemented. The proposed methodology is compared with LSB based steganography technique.[4] From the results, it can be observed that the proposed technique gives better performance than the LSB technique in terms of the PSNR and MSE values.

In general, it is more suitable to obtain a low in MSE values and a high of PSNR values. These values indicate the better quality of the output image. The LSB technique gives high values of MSE irrespective of the inputs. In all the types of images, the proposed methodology produces a better result. Hence, the calculation based on PSNR is also suitable for the proposed methodology.

TABLE II. Accuracy Estimation based on PSNR and MSC

Image	PSNR	MSE	PSNR(LSB)	MSE (LSB)
Image 1	58.0288	0.1076	57.1268	0.1184
Image 2	62.0198	0.1184	60.0918	0.1390
Image 3	61.1187	0.2317	60.0435	0.2106
Image 4	59.0198	0.1296	58.0211	0.1093
Image 5	60.0139	0.2264	58.9131	0.2142

The significances of the proposed methodology over the existing are as follows:

1) The number of messages that can be hidden is greater than the existing methods.

2) The efficiency is Greater since the proposed methodology process with each and every pixel of the total image.

3) Better quality and security is obtained when compared with the LSB technique.

4) The proposed methodology obtains a high PSNR and less MSE values when compared to the existing methodologies.

V. Conclusion and Future Enhancements

A novel steganographic technique is proposed using the fuzzy logic to embed the secret message in the carrier image is performed in this paper. The proposed technique can produce better results when compared to the existing LSB based steganographic techniques with respect to the number and size of messages that can be hidden. This method also performs well in terms of the time taken to retrieve the hidden information from the carrier image as well as in the quality of the retrieved image. Based on the results obtained, it can be observed that the proposed methodology gives better results for hiding the secret information in an image when compared to the existing LSB based steganographic techniques. It also gives additional security for hiding the secret message in an image by calculating the Correlation value in the pixel present in the original as well as in the secret information. The performance is shown by the increased PSNR and decreased MSE values which are obtained for the tested images. Future enhancement in this work is to propose a feature extraction process in order to enhance the security and also to reduce the time taken to process the complete scenario.

References

[1] Image definition, Gonzalez, Woods – Digital Image Processing.

[2] Z Neil F. Johnson and Sushhil Jajodia. “Steganalysis: The Investigation of Hidden Information” - Proceedings of the IEEE Information Technology Conference, Syracuse, New York, USA, 1998.

[3] I.Aveibas, N.Memon, B.Sankur. “Steganalysis based on image quality metrics” - Multimedia Signal Processing, 2001 IEEE Fourth Workshop on, 2001.

[4] A.S.Abdullah, “Text Hiding Based On Hue Content In HSV Color Space”, International Journal of Emerging Trends & Technology in Computer Science, vol. 4, Issue 2, pp. 170-173, March 2015.

[5] AL-Ani, Z.K., Zaidan, A.A., Zaidan, B.B., and Alanazi, H.O., “Overview: Main Fundamentals for Steganography,” Computer Engineering, vol.2, pp.158-165, 2010.

[6] Petitcolas, F.A.P., Anderson, R.J., and Kuhn, M.G., “Information hiding-a survey,” In Proceedings of the IEEE , vol.87, no.7, pp.1062- 1078, 1999.

[7] Craver S., Yeo B.-L., and Yeung M., “Technical trials and legal tribulations.” Communications of the A.C.M., vol.41, no. 7, pp. 44-54, 1998.

[8] Anderson, R.J. and Petitcolas, F.A.P., “On the limits of steganography,” IEEE Journal on Selected Areas in Communications, vol.16, pp.474-481, 1998.

[9] Cheddad A., Condell J., Curran K., and Mc Kevitt P., “Digital image steganography: Survey and analysis of current methods,” Signal Processing, vol.90, pp.727-752, 2010.

[10] Johnson N.F. and Jajodia S., “Exploring steganography: seeing the unseen,” IEEE Computer, vol. 31, no. 2, pp. 26–34, 1998.

[11] Bender W., Butera W., Gruhl D., Hwang R., Paiz F.J., and Pogreb S., “Applications for data hiding,” IBM Systems Journal, vol.39, no.3 & 4, pp.547–568, 2000.

[12] Petitcolas F.A.P., “Introduction to information hiding,” In: Katzenbeisser S., Petitcolas F.A.P. (Eds.), Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Inc., Norwood, 2000.

[13] Miaou S., Hsu C., Tsai Y., and Chao H., “A secure data hiding technique with heterogeneous data-combining capability for electronic patient records,” in: Proceedings of the IEEE 22nd Annual EMBS International Conference, pp. 280–283., 2000.

[14] Fujitsu Ltd., “Steganography technology for printed materials (encoding data into images),” Tackling new challenges, Annual Report 2007, Fujitsu Ltd., pp.33, 2007, Access at: http://www.fujitsu.com/downloads/IR/annual/2007/all.pdf.

[15] Provos N. and Honeyman P., “Hide and seek: an introduction to steganography,” IEEE Security and Privacy, vol.1, no.3, pp.32–44, 2003.

[16] Khursheed F. and Mir A.H., “Fuzzy logic-based data hiding,” In Proceeding of Cyber Security, Cyber Crime, and Cyber Forensics, Department of Electronics and Communication, National Institute of Technology, Srinagar, India, 2009.

[17] Mir A.H., "Fuzzy entropy based interactive enhancement of radiographic images," In Journal of Medical Engineering and Technology, vol.31, no.3, pp.220–231, 2007.

[18] Munirajan V.K., Cole E., and Ring S., “Transform domain steganography detection using fuzzy inference systems,” In Proceeding of IEEE Sixth International Symposium on Multimedia Software Engineering, pp.286- 291, 2004.

[19] Toony Z., Sajedi H., and Jamzad M., “A high capacity image hiding method based on fuzzy image coding/decoding,” In *14th International ‘Computer Society of Iran’ Computer Conference (CSICC’09)*, pp.518-523, pp.20-21, 2009.

[20] Hussain H.S., Aljunid S.A., Yahya S., and Ali F.H.M., “A novel hybrid fuzzy-SVM image steganographic model,” In *Proceeding of International Symposium in Information Technology*, vol.1, pp.1-6, 2010.

[21] Goodarzi M.H., Zaeim A., and Shahabi A.S., “Convergence between fuzzy logic and steganography for high payload data embedding and more security,” In *Proceedings of 6th International Conference on Telecommunication Systems, Services, and Applications*, pp.130-138, 201.