Computerised Information Security Using Texture Based Fuzzy Cryptosystem

Abdulrahman Abdullah Alghamdi
College of Computer Science and IT,
Shaqra University,
Saudi Arabia
alghamdia@su.edu.sa

Abstract—**The main objective of this study is to form a unique and economical steganographic technique for digital pictures employed for secret transmission using texture and fuzzy logic. This technique is employed to embed data in the carrier image and to extract the hidden message within the same carrier image. Initially, fuzzification, which transforms the carrier and the secret image into numerous bitplanes, is completed. Pixel number calculation is completed in the original image. Then, feature extraction is completed in the secret image. Finally, pixel merging follows within the sender region by assigning white and black pixels in the original image and in the secret image. Pixel numbers and texture features are extracted and can be used as a key for retrieving the embedded image from the receiver. This modified approach can be applied in various images. Experimental results reveal that this method will hide and retrieve the secret messages in a carrier accurately.**

Keywords-information security; fuzzy logic; texture features; carrier image; secret image; steganography

I. INTRODUCTION

Maintaining secrecy and security of confidential data over the internet and cloud is very important. Cryptography and steganography are techniques which can be used together to maintain security and secrecy of highly confidential data over the computing environment. Steganography is the method of providing information security for secret images by inserting the message in other messages (carrier images). The proposed methodology provides more than one level of security since it combines value and texture features of all the pixels present in the entire image. Steganography is finalized with numerous enhancements in medium and within the secret pictures. Data hidden in images are most commonly used as input [2, 3]. In this case, the medium which is concealing the data is a picture. The picture will be outlined as a two-dimension coordinate function f(x,y), where x and y represent the coordinates, and f the intensity [1]. During this process, the picture is considered as a matrix of two dimensions.

Regarding the proposed methodology, the text that is to be embedded in a picture is a grey image. Embedding will be done by the application of fuzzy rules on the region merging process. The embedded text will be retrieved simply by the receiver who is aware of the defuzzification method. The most significant part this methodology is that it can be used by any end user. This technique only concentrates on the image's ability of carrying hidden data.

II. LITERATURE SURVEY

Many techniques for information hiding were proposed in [4-6, 8-10, 11-15, 18, 20]. Authors in [16, 17] proposed a method for information hiding. They tried to hide the data using a domain supported fuzzy logic-based methodology. The benefit of this methodology is that it is computationally less complicated compared to existing data hiding strategies. However, the information which is to be hided is sensitive in nature and it's easy to be destroyed by creating a little amendment within the overall data and by dynamical with none explicit visibility. Author in [4] proposed a methodology for the replacement of data in an image. Secret information is hidden as an image by employing a fuzzy based method and cryptography technique which creates minimum distortion within the entire image which ends up in a high quality stego image. The main advantages of this methodology are that it yields a better rate in embedding information and it improves overall security. Authors in [18] designed a strategy supported by the mix of a hybrid fuzzy c-means formula and SVM for proposing steganography. Their model creates an activity such that the key messages are convertible. Authors in [3] developed a replacement schema for steganography by least bit technique for utilizing the hybrid-based edge detector technique. Their technique uses a combination of character detection methodology and edge detection algorithms supporting fuzzy logic. This methodology overcomes the existing methods of steganalysis systems. It additionally generates prime quality stego pictures.

Every steganography-based technique has its own disadvantages. Authors in [12] worked on the various disadvantages of already used steganography systems. Authors in [7] elaborated three kinds of steganographic attacks: in hardiness, in presentation, and in interpretation. Most of the prevailing works used threshold based algorithms, fuzzy C means algorithms, and neural networks-based algorithms. Also, it has been observed that most of the existing methods show less accuracy in hiding images with more information. Therefore, a new methodology to embed secret messages in a carrier image more effectively is necessary.

III. Proposed Methodology

A combination of texture and fuzzy logic-based pixel merging methodology is proposed for embedding information as an image into a carrier image. This combination makes an effective process of steganography, while the quantity of the secret information can be augmented. The proposed methodology is a combination of processing biplanes, texture features of an image and fuzzy rules applied to both original and secret images. The proposed architecture is shown in Figure 1.

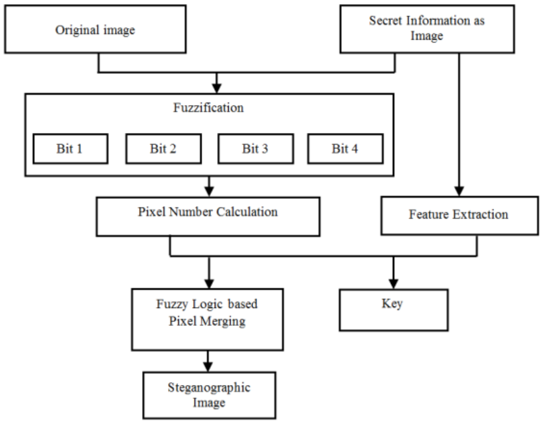

Fig. 1. Architecture of the proposed method

A. *Steganographic Image Generation*

The planned technique consists of the subsequent steps:

- Grey scale original and secret images are considered as input pictures.
- The algorithm counts the amount of black and white pixels in each input picture.
- Input pictures are separated into four monochrome pictures in order to get the bit values from every bitplane.
- The bit pair representing the background is referred to as “lower nibble” and the remaining pair of bits that represents the foreground image is referred as “upper nibble”.
- Pixel merging is completed within the sender area by distributing the white and black pixels to the first image using fuzzy logic by scrutinizing the pixels in the original and secret image. It conjointly calculates pixel range from both images.
- Textural features are additionally calculated for the complete images starting from the first pixel. This process is employed to generate the key for encrypting the hidden image.
- Finally, the obtained area of pixels comprises the steganographic image.

B. *Fuzzification*

Fixing the values of one set of crisp value to a different fuzzy set of qualitative illustration is termed as fuzzification. In several fuzzy strategies like fuzzy based process, fuzzy C-means and fuzzy based reasoning, intensity transformation of values towards various numerals is processed in the initial stage. In the current study, the fuzzification method is the formation of four bitplanes as shown in Figures 2(a), 2(b) and 2(c). The input could be a monochrome image which contains black and white pixels.

C. *Pixel Number Calculation*

Pixel number is computed in order to find the place in the original image where a pixel of the secret image can be incorporated. It is used for decoding the secret message from stego image.

D. *Feature Extraction*

Texture provides some necessary information concerning the structural arrangement of varied surfaces in an image. Texture features accustomed in a unit area can classify the different types of pixels in an image. Grey level co-occurrence matrix (GLCM) options are calculated for the image border regions. For this, features such as correlation, energy, contrast, homogeneity are calculated.

E. *Description of the GLCM Features*

In this method, gray level co-occurrence matrix properties like entropy, energy, contrast and homogeneity are computed. The four GLCM properties used in this method are:

1) Energy

The energy returns the sum of the squared elements in GLCM. The Energy ‘E’ can be calculated by using (1):

$$\sum_{i,j} p(i,j)^2 \tag{1}$$

2) Homogeneity

Homogeneity is a value that counts the closeness of the elements in the GLCM to the its diagonal. Homogeneity ‘H’ is computed by using (2):

$$\sum_{i,j} \frac{p(i,j)}{1+|i-j|} \tag{2}$$

3) Contrast

Contrast computes the intensity between a pixel and its neighbors for the entire image. The contrast ‘Co’ of a pixel can be computes as:

$$Co = \sum_{i,j} |1-j|^2 \, p(i,j) \tag{3}$$

4) Correlation

Correlation computes how a pixel is correlated to its neighbor for the entire image. The correlation ‘Cr’of an image can be calculated by (4):

$$\sum_{i,j} \frac{(i-\mu j)(j-\mu j)P(i,j)}{\sigma_i \, \sigma_j} \tag{4}$$

These features are calculated for the pixels present in the original image and in the secret image. An intruder who intends to modify the hidden data can’t predict or calculate the feature values of the image. This ensures that the information cannot be deciphered by intruders.

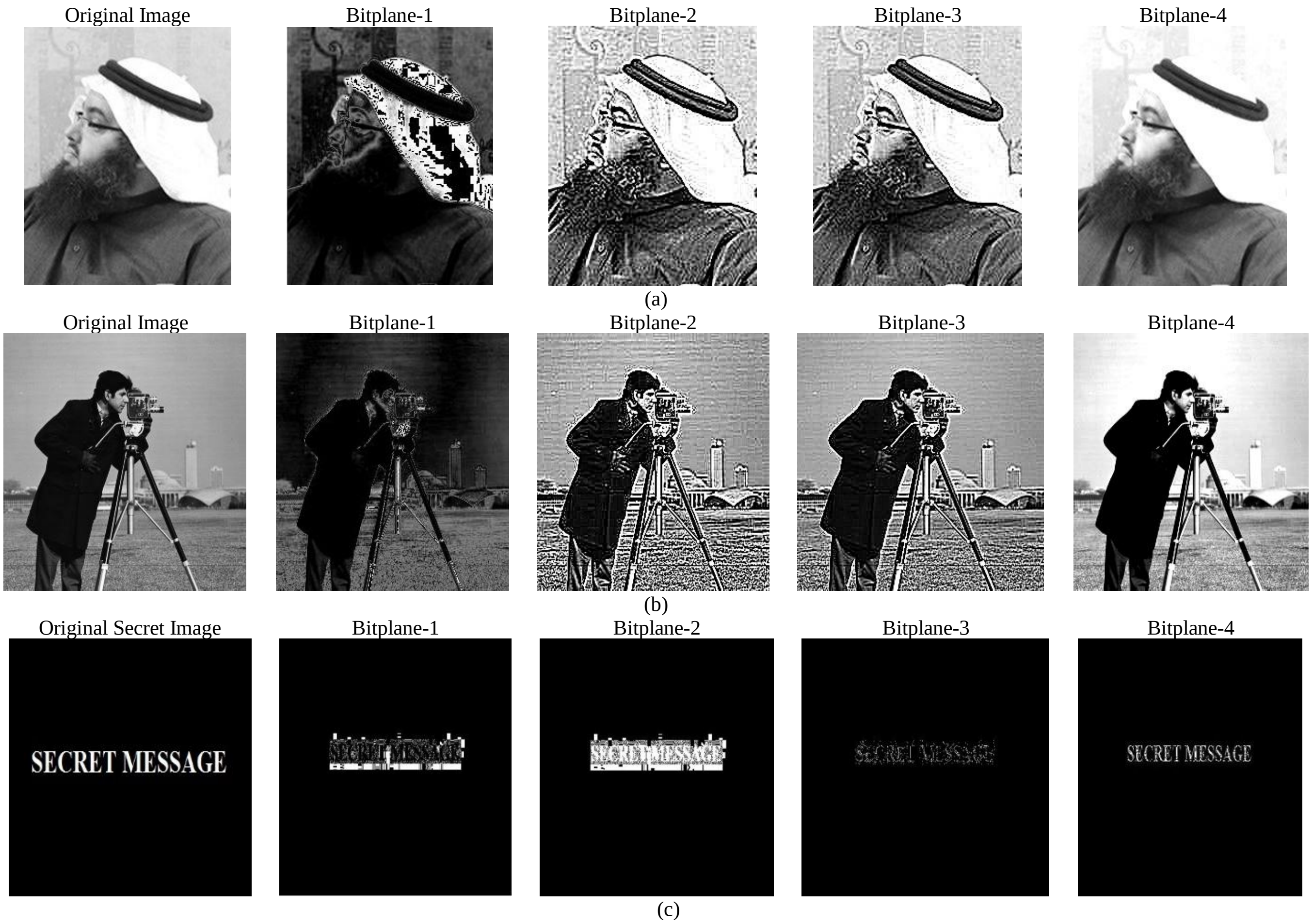

Fig. 2. Fuzzification of (a) a real world original image, (b) a Matlab database image (© M.I.T.) and (c) a secret information image and their bit planes

F. Fuzzy Rules for Pixel Merging

Pixel merging is the method of merging two or more pixels, and here it is completed with the support of fuzzy rules. Four rules where set for this method. This method compares the pixels of original and secret image and hides the key image in the original image. All the fuzzy rules begin the iteration from the initial pixel of the original and 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 of the original image.
- **Fuzzy Rule 2:** If the pixel in O is w and the pixel in S is b then, calculate the pixel number and correlation value of the entire pixels of the original image. Then merge the pixel of S with the one of O. After merging, go to the next pixel in both images.
- **Fuzzy Rule 3:** If the pixel in O is w and the pixel in S is b, then go to the next pixel in S.
- **Fuzzy Rule 4:** If the pixel in O is b and the pixel in S is b, then go to the next pixel in both original and secret image.

G. Encoding the Message

The pixel number of the original image combined with the feature values are the key which is given to the receiver. The receiver will extract the hidden data from the original image by distinction of the proper pixel and by subtracting the texture feature values from it. Since the pixels combined with the texture feature values are taken into account as a key for extracting the hidden data, this method is considered as secure in comparison with different existing steganographic techniques.

IV. Results and discussion

This methodology uses Matlab. The results were obtained by giving the input image along with the carrier image. From the obtained results, it can be noted that the carrier and also the output stego image were indistinguishable visually as shown in Figure 3. The efficiency of this technique is decided from the peak signal to noise ratio (PSNR) and the mean square error (MSE). MSE and the PSNR are the metrics used for scrutinizing the quality of a picture. In general the quality of the processed image is high when the PSNR is high. Low MSE means then the error between the processed and the original image is low. These parameters are outlined as:

$$PSNR = 10\, log_{10}(R^2/MSE\,) \qquad (5)$$

where, M and N are the number of rows and columns in the input images. The MSC value is calculated by using (6):

$$MSE = \frac{\sum_{M,N}[I_1(m,n)- I_2(m,n)]^2}{M*N} \qquad (6)$$

Table I presents the accuracy obtained from the PSNR and MSE values for a few sample data as secret original images.

The projected methodology is compared with LSB based steganography technique [4] and the existing method described in [19]. Results ascertained that the proposed technique offers higher performance than the LSB and the existing technique.

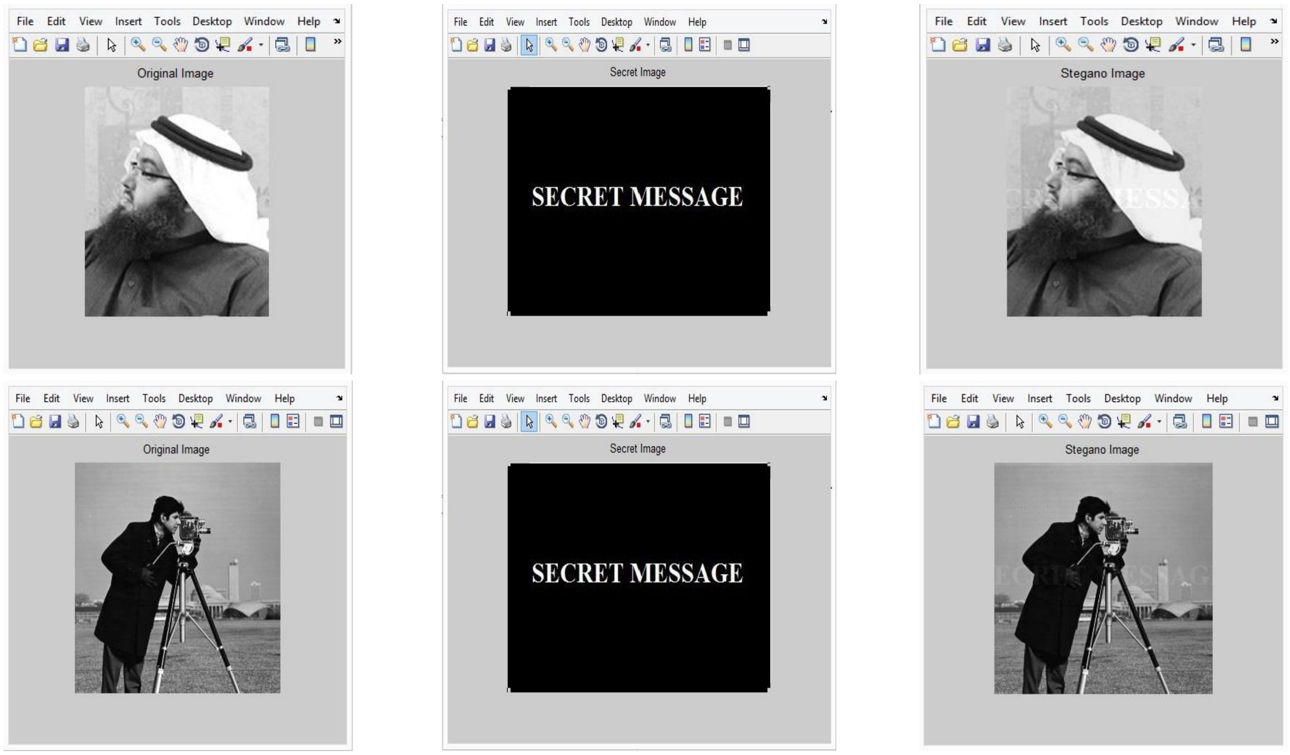

Fig. 3. Results of the original and stegano image for real world and database images

TABLE I. ACCURACY BASED ON PSNR AND MSC

Image	PSNR (Existing method)	MSE (Existing method)	PSNR (LSB based method)	MSE (LSB based method)	PSNR (Proposed method)	MSE (Proposed method)
Image 1	53.0288	0.1176	52.1268	0.1184	57.1268	0.1044
Image 2	59.0198	0.1084	57.0918	0.1390	62.0918	0.0190
Image 3	61.1187	0.2217	61.0435	0.2306	62.0435	0.1106
Image 4	57.0198	0.1196	54.0211	0.1293	54.4101	0.0293
Image 5	58.0139	0.2164	56.9131	0.2142	59.8731	0.1142

V. CONCLUSION

A modified steganographic technique is proposed in order to insert a secret message in a carrier image. The proposed technique can obtain better results than the LSB based and existing steganographic techniques regarding the quantity and the size of the hidden message. This methodology performs well in terms of required time to retrieve the hidden data from the carrier image. The obtained results reveal that this methodology offers better results in concealing a large number of pixels in an image. This methodology offers improved efficiency and accuracy when compared to the existing methods. It additionally offers extra since the texture features of the original and the secret image are combined. The performance of the proposed method can be revealed by the higher PSNR and lower MSE values for different images.

REFERENCES

[1] R. C. Gonzalez, R. E. Woods, Digital Image Processing, Pearson, 2008

[2] N. F. Johnson, S. Jajodia, “Steganalysis: The Investigation of Hidden Information”, IEEE Information Technology Conference, Information Environment for the Future, Syracuse, New York, USA, September 3, 1998

[3] I. Avcibas, N. D. Memon, B. Sankur, “Steganalysis based on image quality metrics”, IEEE Fourth Workshop on Multimedia Signal Processing, Cannes, France, October 3-5, 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, No. 2, pp. 170-173, 2015

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

[6] F. A. P. Petitcolas, R. J. Anderson, M. G. Kuhn, “Information hiding-a survey”, Proceedings of the IEEE, Special Issue on Protection of Multimedia Content, Vol. 87, No. 7, pp. 1062-1078, 1999

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

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

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

[10] N. F. Johnson, S. Jajodia, "Exploring steganography: seeing the unseen", Computer, Vol. 31, No. 2, pp. 26-34, 1998

[11] W. Bender, W. Butera, D. Gruhl, R. Hwang, F. J. Paiz, S. Pogreb, "Applications for data hiding", IBM Systems Journal, Vol. 39, No. 3-4, pp. 547-568, 2000

[12] F. A. P. Petitcolas, "Introduction to information hiding", in: Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Inc., Norwood, 2000

[13] S. G. Miaou, C. M. Hsu, Y. S. Tsai, H. M. Chao, "A secure data hiding technique with heterogeneous data-combining capability for electronic patient records", 22nd Annual International Conference of the IEEE Engineering in Medicine and Biology Society, Chicago, USA, July 23-28, 2000

[14] Fujitsu Ltd., Tackling New Challenges, Annual Report 2007, Fujitsu Ltd., 2007

[15] N. Provos, P. Honeyman, "Hide and seek: an introduction to steganography", IEEE Security and Privacy, Vol. 99, No. 3, pp. 32-44, 2003

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

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

[18] V. K. Munirajan, E. Cole, S. Ring, "Transform domain steganography detection using fuzzy inference systems", IEEE Sixth International Symposium on Multimedia Software Engineering, Miami, USA, December 13-15, 2004

[19] A. A. Alghamdi, "Computerized Steganographic Technique using Fuzzy Logic", International Journal of Advanced Computer Science and Applications, Vol. 9, No. 3, pp. 155-159, 2018

[20] A. A. Alghamdi, "Information Security using Steganographic Method: Genetic Algorithm and Texture Features", Indian Journal of Science and Technology, Vol. 11, No. 34, pp. 1-6, 2018