Contents lists available at Science-Gate

International Journal of Advanced and Applied Sciences

Journal homepage: http://www.science-gate.com/IJAAS.html

Information security and steganography technique for data embedding using fuzzy inference system

Abdulrahman Abdullah Alghamdi *

College of Computing and IT, Shaqra University, Shaqra, Saudi Arabia

ARTICLE INFO

Article history:
Received 22 October 2018
Received in revised form
7 January 2019
Accepted 8 January 2019

Keywords:
Steganography
Fuzzy inference system
Mamdani model
Information hiding
Computer security

ABSTRACT

Steganography is one among the suggestions that can be used to store the secured information in images. Several techniques which follow serial embedding techniques take longer to embed the information. The goal of this paper is to hide the secret image with different resolutions in a carrier image with more accurately aid in less execution time. To realize this goal, the combination of texture and Fuzzy Inference System (FIS) is employed. In the FIS, the fuzzifier converts the crisp input to fuzzy values through membership functions. Texture features are extracted using the Grey Level Co-occurrence Matrix features. Three Membership Functions such as texture features, Edge sensitivity and the Brightness sensitivity are generated and given as input towards the fuzzy system. The Mamdani FIS algorithm is used for embedding the image. All the pixels which are present in the image square is embedded in parallel rather than one by one operations since, it reduces the overall embedding time. By this proposed system, the embedding time is reduced when compared to different existing algorithms. By using this Mamdani based FIS, the peak signal to noise magnitude relation obtained is more for all the pixels present in the image is used for testing.

1. Introduction

Information hiding in digital images was born with advent of the digital technology, steganography techniques where used nowadays in various digital Medias such as the text, image, audio, video etc. Novel steganography techniques work on hiding the data using modern media. Image Steganography is the process of hiding the information present in one image in another image by combining it in to each other. The information which is encoded is called as the cipher text. This is unclear in nature so that the hacker cannot trace it. Cryptography provides security for the data which is hidden in information by applying various novel encryption or decryption techniques. The major role of an Image steganography is to hide and maintain the safe transmission of data by concealing it inside a different data file. It can be done by concealing an image and to prevent a hacker from extracting the data which is hidden. A novel steganography technique for hiding images has been proposed in this paper. A novel method proposed by Sajasi and Moghadam (2013) uses Fuzzy Inference System (FIS) by combining the Mamdani FIS with the Human Visual System (HVS) properties. Alvi and Dawes (2013) proposed a method for hiding the secret data by transforming it into in to fuzzy domain. In their method, two image processing based techniques such as the edge detection and texture feature extraction are done for each fuzzy based pixel. Then, a Least Significant Bit based steganography substitution method is employed for hiding the information in another image. Their method obtained a good accuracy in hiding the information more effectively. Application of the LSB Algorithm in GPU was proposed by Darshan et al. (2014), depicts a method for obtaining the steganography using the method called the computer based unified device by making the computations parallel in nature to a single pixel. It can be done by a novel method of passing the message and shared memory so that it can reduce the overall time taken to execute the algorithm.

The basic approach to compute color image derivatives is to calculate separately the derivatives of the channels and add them to produce the final color gradient. However, the derivatives of a color edge can be in opposing directions for the separate color channels. Therefore, a summation of the

* Corresponding Author.
Email Address: alghamdia@su.edu.sa

https://doi.org/10.21833/ijaas.2019.03.002

Corresponding author's ORCID profile:
https://orcid.org/0000-0002-9976-5016

2313-626X/© 2019 The Authors. Published by IASE.

derivatives per channel will discard the correlation between color channels (Forrest, 1993). As a solution to the opposing vector problem, he proposed the color tensor, derived from the structure tensor, for the computation of the color gradient. Adaptations of the tensor lead to a variety of local image features, such as circle detectors and curvature estimation (Long et al., 2015; Noh et al., 2015; Badrinarayanan et al., 2017; Kendall et al., 2015). In this chapter, we study on methods and techniques to combine derivatives of the different color channels to compute locale image structures.

Al-Rubbaiy (2011) proposed a novel method for hiding the secret data using fuzzy based technique for increasing the robustness of hidden data. Fuzzy based pixel matching algorithm is used in their method. Alghamdi (2018a) proposed a new improved algorithm for hiding the secret data by using the concept of fuzzy logic. His method obtained a good accuracy in hiding the information more effectively. The key aim of this method is to boost the encoded information more effectively by integrating the GA and texture features for achieving the accuracy in information hiding. The process such as a detailed study about various cryptography-based techniques, recent image based steganographic techniques, proposal and design of an improved steganographic method is done.

2. Literature survey

The steganography-based information hiding can be categorized into transform based and domain-based methods (Silman, 2001). In the transform-based method, the data is encoded initially and then it is hided with the cover image. The transform-based method hides messages in additional areas of the image, and this initiates the cover image to separate into priority-based techniques such as high, middle and low. The foremost important character of those strategies is, this method is best against various attack in images. In the Domain based strategies, messages are encoded within the intensity of the pixels. Least-significant bit (LSB) was proposed by Ker (2004) and Mahdavi et al. (2008) is an example of the domain-based techniques.

Xu et al. (2010) developed a novel method for steganography using the hybrid-based edge detector technique. Their technique uses the combination of character detection methodology and edge detection algorithms. This methodology overcomes the existing methods for steaganalysis systems. It additionally generates the prime quality stego pictures. Every steganography-based technique has its own disadvantages. Katzenbeisser and Petitcolas (2000) proposed a methodology which overcomes the various disadvantages of already used steganography systems. Modification of information in an image medium is termed as steganographic attacks. These are often delineated in several forms that can be predicated on numerous techniques of knowledge concealment. Cheddad et al. (2010) elaborated three kinds of stego attacks particularly attacks in hardiness, attacks in presentation, and attacks in interpretation.

From the works found in the literature, it's been ascertained that most of the prevailing works used. Threshold based algorithms; Fuzzy C means algorithms, neural networks-based algorithms. However, just in case of medical applications, the accuracy provided by numerous phases of segmentation isn't enough to form effective selections. Also it has been observed that most of the existing methods show less accuracy in hiding the images which has more information. Hence, a novel methodology for embedding the secret data in a carrier image more effectively is necessary.

3. Proposed methodology

The elements of the planned model as shown in Fig. 1 are represented as follows. The message that is needed to cover is considered as the Data for Input. Therefore, the proposed system uses the required file formats so that the data created as input to the system may be in any format. However, if the data is big, then it cannot be hidden on tiny image. Compression is performed in larger data and it can be considered as a key image. The proposed system for embedding the data in the form of image or text can be done using the fuzzy inference system. Initially, an image as data is given as input towards the proposed system. In order to encrypt the input secret data, the data should be either in the form of text or image. Then the cover image is split into 9 blocks. In the Feature extraction process; each of the block input to FIS. Then, Extract the Texture feature, the Edge sensitivity and the Brightness sensitivity. Form the fuzzy inference system using the Mamdani FIS (Mamdani and Assilian, 1975). The algorithm for embedded input text is as follows:

Step 1. Encrypt the secret data which is given as input. It can be either text or image.
Step 2. Divide the cover image into 9 blocks.
Step 3. Perform the Feature extraction from each block.
Step 4. Give the blocks as input to FIS.
Step 5. Perform Feature extraction process

- Step 5.1 Perform the Texture feature extraction process.
- Step 5.2 Perform the Edge sensitivity Extraction process
- Step 5.3 Perform the Brightness sensitivity Extraction process

Step 6. Compute the Fuzzy Inference System

3.1. Extracting texture feature

Color Feature extraction in pixels is the process of extracting the color features which are necessary for identifying the color characters of each pixels. Among them, some of the features such as RGB, CYANY, Monochrome are computed in this paper.

The color properties used in this method are as follows.

3.2. Color invariance feature

In this section, the dichromatic reflection model is explained Shafer (Mamdani and Assilian, 1975). The dichromatic reflection model explains the image formation process and therefore models the photometric changes, such as shadows and secularities. On the basis of this model, methods are discussed containing invariance.

3.3. Dichromatic reflection feature

The Dichromatic Reflection Model (Forrest, 1993) divides the light that falls upon a surface into two distinct components: specular reflection and body reflection. Specular reflection is when a ray of light hits a smooth surface at some angle. The reflection of that ray will reflect at the same angle as the incident ray of light. This kind of reflection causes highlights. Diffuse reflection is when a ray of light hits the surface which will be reflected back in every direction. Suppose we have an infinitesimally small surface patch of some object, and three sensors are used for red, green and blue.

3.4. Optimization algorithm

Particle Swarm Optimization: This algorithm was proposed by Kennedy (1995). This algorithm is mainly inspired from behavior of bird flocking searching for food. Each particle in the pool represents a solution. These particles are mass less / volume lessor of small mass / volume. Each particle has its position and velocity in the pool. This position and velocity is updated relative to other particle's position and velocity and its own previous position and velocity.

These features are calculated for all the pixels present with in both the original key image. An intruder who intends to modify the hidden data can't predict or calculate the feature values of the image wherever the information perhaps hidden. This ensures that the information cannot be hacked by any intruders.

3.5. Fuzzy inference system

In the fuzzy inference system, all the inputs are extracted as values from feature extraction. Four Membership Functions from the texture features, Membership Functions from the Edge sensitivity and the Membership Functions from the Brightness sensitivity are given as input towards the fuzzy system. The fuzzy inference engine is proposed next to the fuzzy inference system which has a Mamdani type. A fuzzy operator AND is used for combining the antecedents present in it. Aggregation is formed by combining the fuzzy rules and implication method. Followed by a de-fuzzifier which converts the fuzzy output into a crisp value. All the above process can be carried out sequentially.

To calculate the FIS, following steps has to be done with the inputs from feature extraction process

1. Define the fuzzy rules.
2. FIS can be fuzzified from the inputs obtained from feature extraction process.
3. Combination of fuzzified inputs based on fuzzy rules for defining fuzzy functions.
4. Formation of implication by combining the rule and the output membership function.
5. Formation of aggregation by combining the fuzzy rules and implication.
6. Defuzzification can be done when a crisp output is needed.

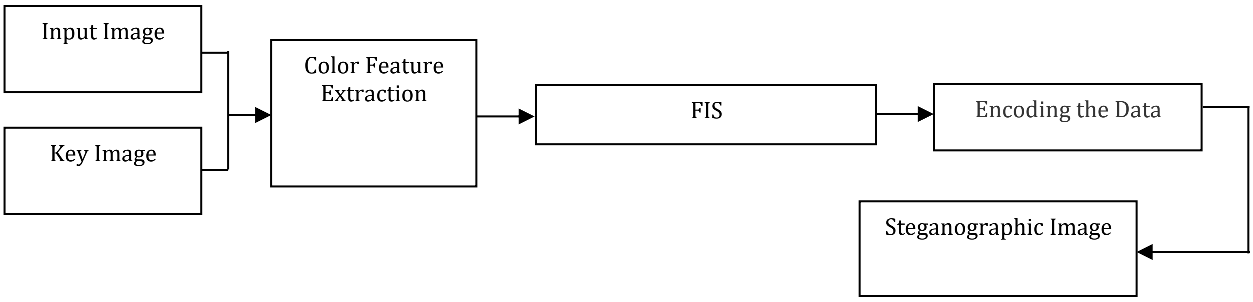

Fig. 1: Architecture of the proposed model

3.6. Extracting the hidden text

For extracting the hidden text present in the image, reverse the process of the fuzzy inference system based embedding process. Extract the confidential data which is hidden in the stego image from sequentially since the overall embedding process is done sequentially. This process is called as defuzzification.

4. Experimental results and discussion

The PSNR and MSC values obtained for the metrics in equation 5 and 6 for the proposed Fuzzy Inference System decides the overall accuracy. It is the combination of the Mamdani FIS with texture features for variable original cover image of resolutions such as 128X128, 256X128, 256X256 and 384X256 where used for embedding. It is shown in Table 1. Based on the resolution, the proposed method generates a good quality of result as shown in Fig. 2 and also PSNR values. From the results obtained, it can be revealed that the information hiding capability can be more for the proposed methodology. When compared to the works done by Alghamdi (2018b) the proposed approach obtains an increased in PSNR values. The MSE and also the PSNR are the metrics used for scrutinizing the quality of a picture. In general, the upper PSNR, the higher quality of the processed image. MSE is that the accumulative square error that lies between the processed and also the original image, furthermore PSNR is that the live of peak error. Once the MSE price is low, then the error is additionally Low. These parameters are outlined as follows:

$$PSNR = 10\ log_{10}(R^2/MSE\ ) \tag{1}$$

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:

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

For a sample of size n, with the n raw scores X_i, Y_i, the Spearman's rank correlation is defined as follows

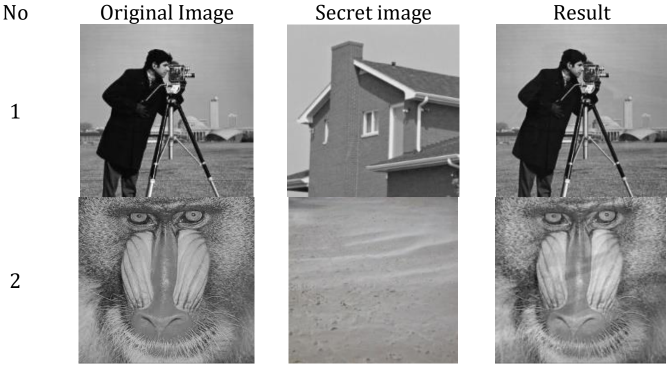

Fig. 2: Proposed outputs

Table 1: The comparison results based on PSNR values between the proposed and existing methods

Secret Image	Baboon Image		Lena Image	
	PSNR for Existing Method	PSNR for Proposed Method	PSNR for Existing Method	PSNR for Proposed Method
128X128	60.2784	61.2404	59.7247	60.6624
256X128	57.343	57.8787	56.9629	58.9791
256X256	54.2562	56.2837	54.0827	56.0924
384X256	52.749	54.7845	52.6082	53.9215
Secret Image	Baboon Image		Lena Image	
	Spearman's rank correlation for Existing Method	Spearman's rank correlation for Proposed Method	Spearman's rank correlation for Existing Method	Spearman's rank correlation for Proposed Method
128X128	1.3076	1.2134	2.2014	2.2083
256X128	1.2184	1.2270	2.1130	2.2180
256X256	1.1117	1.3216	2.2126	2.2186
384X256	1.0096	1.4283	2.1133	2.4193
Secret Image	Baboon Image		Lena Image	
	PSNR for Existing Method	PSNR for Proposed Method	PSNR for Existing Method	PSNR for Proposed Method
128X128	60.2784	61.2404	59.7247	60.6624
256X128	57.343	57.8787	56.9629	58.9791
256X256	54.2562	56.2837	54.0827	56.0924
384X256	52.749	54.7845	52.6082	53.9215

Table 1 shows the comparison results based on PSNR values between the proposed and existing methods. Time taken (in seconds) for two types of images for different sizes are shown in Table 2. Resolutions such as 128X128, 256X128, 256X256 and 384X256 where taken for processing the proposed algorithm.

Table 2: Execution time taken for two types of images (in seconds)

Secret Image	Baboon Image		Lena Image	
	Time Taken for Existing Method (In Seconds)	Time Taken for Proposed Method (In Seconds)	Time Taken for Existing Method (In Seconds)	Time Taken for Proposed Method (In Seconds)
128X128	468	304	547	324
256X128	353	287	629	581
256X256	666	537	827	621
384X256	659	445	582	223

5. Conclusion and future work

A novel Fuzzy Inference System based Steganographic scheme is proposed based on the combination of Features and Fuzzy Inference System. The Mamdani method of fuzzy inference system is used in this paper for FIS in order to obtain a greater accuracy and lesser execution time. From the result obtained, it can be concluded that the proposed Feature based FIS system takes lesser time when compared to the other existing methods. Embedding time is reduced by 20% as compared to other serial embedding based techniques. In this algorithm, the PSNR values obtained is more for all the pixels present in the complete image. The proposed algorithm is tested for images with different resolutions taken from already tested datasets. Future work can be a proposal of further enhanced method that could overcome some of the drawbacks present in this work. This work can be enhanced to support various formats of images such as BMP, JPEG, TIFF and PPM image formats. Moreover, an improved and efficient compression technique can be employed for the process of compressing the image.

Acknowledgement

The author acknowledges with gratitude the support provided by Shaqra University for conducting this research.

Compliance with ethical standards

Conflict of interest

The authors declare that they have no conflict of interest.

References

Alghamdi AA (2018a). Information security using steganographic method: Genetic algorithm and texture features. Indian Journal of Science and Technology, 11(34): 1-6. https://doi.org/10.17485/ijst/2018/v11i34/131381

Alghamdi AA (2018b). Computerized steganographic technique using fuzzy logic. International Journal of Advanced Computer Science and Applications, 9(3): 155-159. http://dx.doi.org/10.14569/IJACSA.2018.090323

Al-Rubbaiy FH (2011). Concealment of information and encryption by using fuzzy technique. Journal of the College of Basic Education, 16(69): 25-34.

Alvi AK and Dawes R (2013). Image steganography using fuzzy domain transformation and pixel classification. In the 25th International Conference on Software Engineering and Knowledge Engineering (SEKE'13): 277-282.

Badrinarayanan V, Kendall A, and Cipolla R (2017). Segnet: A deep convolutional encoder-decoder architecture for image segmentation. IEEE Transactions on Pattern Analysis and Machine Intelligence: 39 (12): 2481-2495. https://doi.org/10.1109/TPAMI.2016.2644615 **PMid:28060704**

Cheddad A, Condell J, Curran K, and Mc Kevitt P (2010). Digital image steganography: Survey and analysis of current methods. Signal Processing, 90(3): 727-752. https://doi.org/10.1016/j.sigpro.2009.08.010

Darshan R, Prabu R, and Divya M (2014). Acceleration of LSB algorithm in GPU. International Journal of Computer Science and Information Technologies, 5(3): 2865-2867.

Forrest S (1993). Genetic algorithms: Principles of natural selection applied to computation. Science, 261(5123): 872-878. https://doi.org/10.1126/science.8346439 **PMid:8346439**

Katzenbeisser S and Petitcolas F (2000). Information hiding techniques for steganography and digital watermarking. Artech house, Norwood, Massachusetts, USA.

Kendall A, Badrinarayanan V, and Cipolla R (2015). Bayesian segnet: Model uncertainty in deep convolutional encoder-decoder architectures for scene understanding. arXiv preprint arXiv:1511.02680.

Ker A (2004). Improved detection of LSB steganography in grayscale image. In the 6th International Conference on Information Hiding, Toronto, Canada: 97-115. https://doi.org/10.1007/978-3-540-30114-1_8

Long J, Shelhamer E, and Darrell T (2015). Fully convolutional networks for semantic segmentation. In the IEEE Conference on Computer Vision and Pattern Recognition, Boston, MA, USA: 3431-3440. https://doi.org/10.1109/CVPR.2015.7298965

Mahdavi M, Samavi S, Zaker N, and Modarres-Hashemi M (2008). Steganalysis method for LSB replacement based on local gradient of image histogram. Iranian Journal of Electrical and Electronic Engineering, 4(3): 59-70.

Mamdani EH and Assilian S (1975). An experiment in linguistic synthesis with a fuzzy logic controller. International Journal of Man-Machine Studies, 7(1): 1-13. https://doi.org/10.1016/S0020-7373(75)80002-2

Noh H, Hong S, and Han B (2015). Learning deconvolution network for semantic segmentation. In the IEEE International Conference on Computer Vision, Santiago, Chile: 1520-1528. https://doi.org/10.1109/ICCV.2015.178

Sajasi S and Moghadam AME (2013). A high quality image steganography scheme based on fuzzy inference system. In the 13th Iranian Conference on Fuzzy Systems, IEEE, Qazvin, Iran: 1-6. https://doi.org/10.1109/IFSC.2013.6675666

Silman J (2001). Steganography and steganalysis: An overview. Sans Institute, 3: 61-76.

Xu H, Wang J, and Kim HJ (2010). Near-optimal solution to pair-wise LSB matching via an immune programming strategy. Information Sciences, 180(8): 1201-1217. https://doi.org/10.1016/j.ins.2009.12.027