ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645
Indian Journal of Science and Technology, *Vol 11(34), DOI: 10.17485/ijst/2018/v11i34/131381, September 2018*

Information Security using Steganographic Method: Genetic Algorithm and Texture Features

Abdulrahman Abdullah Alghamdi*

College of Computing and IT, Shaqra University, Kingdom of Saudi Arabia;
alghamdia@su.edu.sa

Abstract

Objectives: There is an oversized want of web applications that needs the information to be transmitted in a safer method. Steganography and cryptography help in providing information security. Steganography hides the data by inserting the information into another image format. For maintaining the defense of information thrashing and communication over a network, the steganography based anticipated system uses cryptographical based algorithmics by means of Steganography. **Method/Statistical Analysis:** A combination of Genetic Algorithm (GA) along with the texture featuresis employed in this paper for effective information hiding in image wherever the data is to be hidden so that detection of embedded information becomes multifaceted. Initially the feature extraction is done, and it is combined with the GA. **Findings**: Within the anticipated system, the data that we would like to create in a protected form is initially compressed to a shrinkable size so that the compressed information is remodeled into cipher text by applying the combination of GA and Texture features algorithmic program. Experiment results reveal that the proposed combination for steganography obtains more accurate results when compared to the other algorithms. **Application/Improvements:** Future enhancements in the present work would be an enhanced algorithm which can be applied to different types and sizes of images.

Keywords: AES Algorithm; Computer Security, Cryptography, Genetic Algorithm, Steganography, Texture Features

1. Introduction

Cryptography and Steganography, the recent and widely applied algorithm that manages data hiding so as to hide the information more accurately. It is the approach that hides the data present in an image. Steganography hides the messages of by encoding the information in another image. The encoded information called as the cipher text is unclear so that the hacker cannot find it. This work proposed to create a system that uses a combination of GA and GLCM Features for hiding the information in an image more accurately. Existing work tends to hide the data more accurately, there's an opportunity that the hacker might decode the message. Hence, this work is proposed with a lot of security levels and to urge an extremely secured mechanism for concealing the information. This combination can make this method computationally impossible to encode the data. 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

*Author for correspondence

and design of an improved steganographic method, and its performance analysis are done.

2. Literature Survey

The steganography-based information hiding can be categorized into transform based and domain-based methods[1,2]. In the transform-based method, the data is encoded initially and then it is hidden with the cover image. The transform-based method hides the 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 attacks in images. In the Domain based strategies[3], messages are encoded within the intensity of the pixels. Least-Significant Bit (LSB)[4,5] is an example of the domain-based techniques.

In[6] developed a replacement schema for steganography by least bit technique for utilizing the hybrid-based edge detector technique. Their technique uses the combination of character detection methodology and edge detection algorithms which are supported by fuzzy logic. This methodology overcomes the existing methods for steaganalysis systems supported by the methodology of applied mathematical based analysis. It additionally generates prime quality stegopictures. Every steganography-based technique has its own disadvantages. Authors in 7, enhanced 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. In[8] elaborates three kinds of steago attacks particularly attacks in hardiness, attacks in presentation, and attacks in interpretation.

From the works found within 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. Therefore, new and efficient methodology to embed the most important messages in a carrier image more effectively is necessary.

3. Proposed Methodology

Figure 1 shows the operating model of the proposed technique. The elements of the planned model are represented as follows. The message that is needed to be covered is considered as the Data for Input. Therefore, the planned system uses the required file formats so that the data created as input to the system maybe in any format. However, if the data is big, then it cannot be hidden in a tiny image. Compression is performed in large data and it

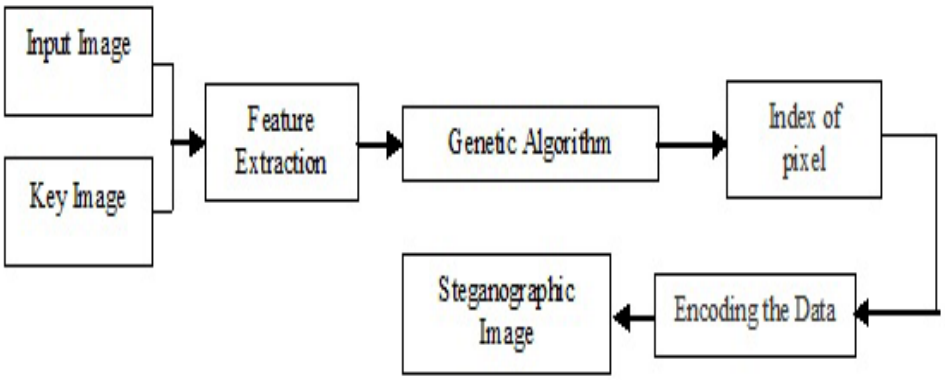


Figure 1. Proposed model.

can be considered as a key image. The compression rule is shown in the AES rule for Cryptography. This reduces the dimensions of the original knowledge that is needed to be covered in a given key image.

3.1 AES Rule for Cryptography

This rule specifies the methodology proposed in 2, in which an interchangeable block cipher that may have data blocks of 128 bits, along with the cipher keys of length 128, 192, and 256 bits respectively. The input, output and the cipher key used in the Rijndael algorithm contains 128, 192 or 256 bits for every bit sequence with the condition that both the input and output sequences have a similar length. The overall length of the input and output bits areof the three predefined values. This can be an exception for the AES where the over all allowed length is 128.

3.2 Feature Extraction

Texture provides some necessary information concerning the arrangement of varied surfaces in an image. Texture features accustomed in an unit area can differentiate the various types of pixels in an image. Grey Level Co-Occurrence Matrix (GLCM)[10] options are calculated for the regions within the border of the images. In general, GLCM creates grey-co matrix by scheming the frequency with that a pixel with grey-level (greyscale intensity) worth 'i' happens horizontally adjacent to a pixel with the worth 'j'. Everypart of (i,j) in GLCM specifies the quantity of times that the pixel with worth 'i' happens horizontally adjacent to a pixel with worth 'j'. For this, features such as correlation, energy, contrast and homogeneity are calculated. The Description of the GLCM features is as follows:

3.2.1 Description of the GLCM Features

In this method, GLCM properties like entropy, energy, contrast and homogeneity are computed. The four GLCM properties used in this method are as follows:

3.2.1.1 Energy

The energy returns the sum of the squared elements in GLCM. The Energy 'E' can be calculated using the formula

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

3.2.1.2 Homogeneity

The Homogeneity is a value that counts the closeness of the pixels in the GLCM to the it's diagonal. Homogeneity 'H' is computed using the formula.

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

3.2.1.3 Contrast

The contrast computes the intensity between a pixel and its neighbor for the entire image. The contrast 'Co' of a pixel can be computes as

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

3.2.1.4 Correlation

Correlation computes how a pixel is correlated to its neighbor for the entire image. The Correlation 'Cr' of an image can be computes as follows

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

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 is perhaps hidden. This ensures that the information cannot be hacked by any intruders.

3.3 Cipher Text

The cipher text which is generated from AES formula is processed once more during this part. Therefore, initially the complete information is regenerated into a four-bit based blocks that are employed to exchange the key image recovered bits of the pixels. Thus, the substitution of LSB is performed based on the idea of four bit instead of three bits. The key image is that the image that is employed to hide the sensitive information. Therefore, that may be

employed in any size depends upon the number of data that's needed to hide in an image. Three main phases such as choice, crossover and mutation where used by the GA. However, the combination of texture feature makes the algorithm to choose the phases randomly when looking for the information as key. Thus, the decoding of input information that is hidden in an image is suspected and this process is done by analyzing the complete row and column of pixels.

3.4 Texture based Genetic Algorithm

Initially, the feature extraction is done within the input and key images. Then, the input image is processed within the rows and used for embedding the information in it. If the information remains to be hidden, then the method encodes the information in column. Hence, the complete image is employed and the choice of random rows of resolution is employed. Algorithm for hiding the data using the combination of texture features and GA is as follows:

- Input: Texture Features, Rows and columns of pixels:
- Choose row M*S index
- Take away selected index and size the image
- Once more compute the index = M*S
- Take away the selected index and adjust the image
- Select the index in rows area using cross over and generate the row of new image
- Compute the low intensity pixel from the sequences
- Hide the information on pixels
- Repeat the process until entire information is hidden within the image.

Index of pixel is applied to hide the information. Therefore, the chosen pixels index is employed to produce reference for an algorithmic rule process. Encoding the Data: Information about the encoded pixels are held individually in rows and columns of the pixels present in the image where the information is to be encoded, so that recovering the output image is easier. Steganographic Image is finally the image which is generated with hidden data as the resultant image.

4. Results and Discussion

In order to validate the overall performance of the proposed technique, many experimental results are carried out and mentioned in this section. The images which are used to test the proposed algorithm are taken from publicly available database8 that is separately shown in Figure 2 and considered as cover images. The image which is shown in Figure 3 is the Steganographic results for cover image 1, 2, 3 and 4 respectively. Table 1 displays the PSNR values derived from the planned technique versus those obtained from the Mielikainen's and our existing technique[11]. From the table, it can be concluded that the

Table 1. Comparative results with existing Steganographic algorithms

Image/ Method	Mielikainen's method	Fuzzy logic-based method	Proposed Method
Cover image 1	52.86139	53.02881	53.15277
Cover image 2	52.41057	52.41983	53.01473
Cover image 3	52.43724	52.83874	53.03539
Cover image 4	52.42461	52.71986	52.93324

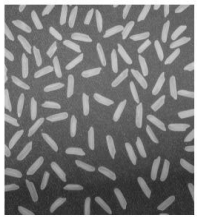
Cover image 1	Cover Image 2	Cover image 3	Cover image 4
			
Secret Image 1	**Secret image 2**	**Secret image 3**	**Secret image 4**
			

Figure 2. Cover images and its corresponding secret image to be embedded.

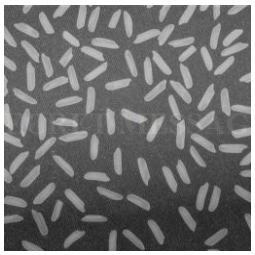
Steganographic Image 1	Steganographic Image 2	Steganographic Image 3	Steganographic Image 4
			

Figure 3. Steganographic results.

proposed technique provides higher PSNR values for various stegopictures compared with existing methods. Hence, the overall quality of the output obtained from our method is more accurate.

From the table, it can be clear that the proposed method achieves more accurate results when compared to two other existing methods for hiding information in images.

5. Conclusion

An automatic method for information hiding is projected in this paper is summarized with the subsequent points: An enhanced method with the mixture of GA and GLCM features victimization Genetic formula is proposed for extremely secured digital communication in close to all types of images. This methodology provides an accurate image quality with no difference in the image since the obtained PSNR Values of Stegnopictures are high. The main advantage of this technique is that the strategy used for information hiding is accurate and therefore the combination of GA and texture features for information hiding is more secure. The proposed system uses the Compression based formula to scale back the dimensions of the input data. As a result less amount and fewer area in image hiding is required.

6. Acknowledgement

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

7. References

1. Soleimanpour-Moghadam M. A novel technique for steganography method based on improved genetic algorithm optimization in spatial domain. Iranian Journal of Electrical and Electronic Engineering. 2013; 9(2):67–75.
2. Silman J. Steganography and steganalysis: An overview. SANS Institute; 2001. p. 1–10.
3. Lee YK, Chen LH. High capacity image steganographic model. IEEE Proceedings of Visual Image Signal Processing. 2000; 147(3):288–94. https://doi.org/10.1049/ip-vis:20000341.
4. Ker A. Improved detection of LSB steganography in grayscale image. International Workshop on Information Hiding; 2005. p. 97–115.
5. Mahdavi M, Samavi Sh, Zaker N, Hashemi M. Steganalysis method for LSB replacement based on local gradient of image histogram. Iranian Journal of Electrical and Electronic Engineering. 2008; 4(3):59–70.
6. Xu H, Wang J, Kim HJ. Near-optimal solution to pairwise LSB matching via an immune programming strategy. Information Sciences. 2010; 1201–17. https://doi.org/10.1016/j.ins.2009.12.027.
7. Petitcolas FAP. Introduction to information hiding. Katzenbeisser S, Petitcolas FAP, editors. Information Hiding Techniques for Steganography and Digital Watermarking. Norwood: Artech House, Inc; 2000.
8. Cheddad A, Condell J, Curran K, Mc Kevitt P. Digital image steganography: Survey and analysis of current methods. Signal Processing. 2010; 90(3):727–52. https://doi.org/10.1016/j.sigpro.2009.08.010.
9. Daemen J, Rijmen V. The block Cipher Rijndael. LNCS-CARDIS. Springer-Verlag Berlin Heidelberg; 1998. p. 277–84.
10. Harralick RM, Shanmugam K, Dinstein K. Textural features for image classification. IEEE Transaction on System, Man and Cybernetics. 1973; 3(6):610–21. https://doi.org/10.1109/TSMC.1973.4309314.
11. Alghamdi AA. Computerized steganographic technique using fuzzy logic. International Journal of Advanced Computer Science and Applications. 2018; 9(3):1–5.