Available online at sjuoz.uoz.edu.krd
Science Journal of University of Zakho
Vol. 7, No. 1, pp. 27–32, Mar.-2019

journals.uoz.edu.krd

p-ISSN: 2663-628X
e-ISSN: 2663-6298

IMAGE STEGANALYSIS IN FREQUENCY DOMAIN USING CO-OCCURRENCE MATRIX AND BPNN

Isamadeen A. Khalifa [a,*], Subhi R. M. Zeebaree[b,c], Musa Ataş [d], Farhad M. Khalifa [e]

[a] Department of Networks, Bardarash Technical Institute, Duhok Polytechnic University, Kurdistan Region, Iraq (Isamadeen.khalif@dpu.edu.krd)
[b] Duhok Polytechnic University, Kurdistan Region, Iraq (subhi.rafeeq@dpu.edu.krd)
[c] Tishk University-College of Engineering-Erbil, Kurdistan Region, Iraq (subhi.rafeeq@dpu.edu.krd)
[d] Department of Computer Engineering, Engineering Faculty, Siirt University, Siirt, Turkey (musa.atas@siirt.edu.tr)
[e] Department of Networks, Bardarash Technical Institute, Duhok Polytechnic University, Kurdistan Region, Iraq (farhad.khalifa@dpu.edu.krd)

Received: Jan. 2019 / Accepted: Mar., 2019 / Published: Mar., 2019 https://doi.org/10.25271/sjuoz.2019.7.1.574

ABSTRACT:
In the last two decades, steganalysis has become a fertile research area to minimize the security risks left behind by Misuse of data concealment in digital computer files. As the propagation of hidden writing increased, the need for the steganalysis emerged and grew to a large extent necessary to deter illicit secret communications. This paper introduces a steganalysis system to detect hidden information in images through using co-occurrence matrix, frequency domain transform, the first three moments, and back propagation neural network (BPNN). Four varieties of the system implemented. Firstly, the co-occurrence matrix calculated for the input image, which suspected to be a carrier of hidden secret information. Second, three levels of discrete wavelet transform (DWT) are applied resulting in 12 subbands. Then, those subbands along with the original image are transformed by discrete Fourier transform (DFT) or discrete cosine transform (DCT) to produce 13 subbands. After that, the first three moments are calculated resulting feature vector with 39 features. Finally, BPNN is used as a classifier to determine whether the image is containing hidden information or not. The system is tested with and without co-occurrence matrix, each of them once using DFT and another time using DCT. The results have shown that using co-occurrence matrix with DFT has the highest performance, which was 81.82% on the Hiding Ratio of 0.5 bit per pixel. This work demonstrates a good effect comparing to previous works.

KEYWORDS: Steganalysis, Co-Occurrence matrix, DWT, DFT, DCT, BPNN.

1. INTRODUCTION

Due to the tremendous development in the field of digital technology, Internet communications, and personal privacy has become more easily violated. There was a need to preserve the confidentiality of personal data when it was transmitted to prevent hackers from accessing it. The beginning of the last decade of the last century saw the emergence of the forefront of research on writing about hidden writing Although hidden writing generally has deep roots in history, various methods of performing hidden writing have used, and some of it primitive [1][2]. The end of the same decade saw the emergence of the first research that attempts to detect hidden writing in digital media. It was the beginning of the science of Steganalysis. Thus opening the wide door for researchers to engage in the fields of hidden writing and steganalysis, and it was a fertile field of scientific research fields and produced countless methods in both fields [3].

Steganalysis is the technique and science that is used to decide if the messages are involved in the image or not by the steganography algorithm. Steganalysis system is utilized to find, extract, disable or change the message before arriving at the recipient [4]. Misuse of hidden writing poses real risks at various levels. The need for "hidden information analysis" has significantly emerged to deter illegal secret communications in order to increase the prevalence of hidden writing. Steganalysis tools are essential for Internet security professionals. Law enforcement agencies need good programs that can identify suspicious files on the computer or the Web [5].

In this paper, a steganalysis system with four verities suggested. The suggested system goals to uncover the presence of a secret message that has embedded into a cover image. Where the reveal task established on previous training of the classifier on the statistical features of a dataset of Stego and clean images, by using supervised learning methods.

The statistical features of the suggested system consist of passing the input images to Co-Occurrence Matrix features of contrast, then applying three levels of DWT using Haar filter. After that taking histogram for each subband, passing to DFT or DCT depending on what verity is used. And calculating first three order moments. Finally using BPNN to classify the image into Stego or clean one. Matlab R2011a used to implement the system.

2. LITERATURE REVIEW

P.Thiyagarajan et al. [6] suggested a global image steganalysis approach which used RGB to HSI color model conversion. The improved global Steganalysis algorithm is tested in Stego-image database which obtained by implementing different RGB Least Significant Bit Steganography algorithms. They suggested using the color conversion system model and visual perception to distinguish between the Stego and the cover image.

Gong and Wang, [7] proposed the steganography detection algorithm based on colors gradient co-occurrence matrix CGCM to the GIF images. CGCM Is built with colors and gradient matrix of the GIF image, and 27-dimensional statistical features of CGCM, Which are between adjacent pixels are sensitive to the color relationship and break the image texture, are extracted.

* Corresponding author

Support vector machine SVM methods make the 27-dimensional statistical features to steganalysis secret message in GIF images. The results mention that the suggested algorithm is effectively more than several GIF steganography algorithms and steganography tools.

In [8] Aljarf, Amin, Filippas, and Shuttelworth proposed a steganography detection system for both color and gray images based on four features which are homogeneity, correlation, contrast, and energy. Using grey images for steganography has many limitations. The first side of work involves making a set of step images. These Stego-images have various image file style. So, these Stego-images have been done using three steganography tools: S-Tools, F5 algorithm, and Open Stego. The Stego-images are utilized to train the detection system in the next step. However, the second side of the work involves detecting the secret message. So the co-occurrence matrix calculated for all images, to detect the hidden data. A number of image features extracted from the matrix. These features are necessary to distinguish between the Stego images and the clean images.

In [9] J. Zeng, S. Member, S. Tan, S. Member, B. Li, and S. Member proposed a general hybrid deep-learning framework for JPEG steganalysis. The proposed structure includes two phases. The first stage is hand-crafted corresponding to the quantization, convolution, and truncation of the rich models. The other phase is a compound neural network in which the parameters learned in the training procedure.

In [10] M. Kaur and G. Kaur reviewed various steganalysis techniques. Steganography and steganalysis have developed. Steganography and steganalysis received a great deal of attention from law enforcement and the media. Many robust and strong methods of steganalysis and steganography, can be considering the methods of steganalysis that are used for this operation. They gave several ideas about steganalysis and its methods.

C. G. Eichkitz, J. Davies, J. Amtmann, and M. G. Schreilechner [11] explained how gray level co-occurrence matrix (GLCM) can be suitable, to do on 3D images of seismic data. (GLCM) Can supply important insight into the subsurface during attribute analysis. Many authors have shown the GLCM is a beneficial tool for the description of seismic facies. Because (GLCM)-based attributes can be calculated in various directions, it can be used to determine directional variations in seismic data. It opens the door to distinguish between sedimentary facies and sample of fracturing, involving the delineation of fractured zones and their strike and dip.

C. Di Ruberto, G. Fodde, and L. Putzu, [12] explored different texture descriptors took out from medical images. For Medical Color Image Classification, various color spaces used. They started by decomposing the color image into three channels Ch1, Ch2, and Ch3, obtaining three various images to extend the classical grey level texture features to color texture features. The classical implementation used and every time passed different color channel to them. The most intuitive way to take into account is color information for the computation of texture feature. The results of the collection is a feature vector nine-times larger than the classical feature vector, consist of three inter-channel feature vector (Ch1, Ch1), (Ch2, Ch2) and (Ch3,Ch3) and six inter-channel feature vector (Ch1, Ch2), (Ch2, Ch1), (Ch1, Ch3), (Ch3, Ch1), (Ch2, Ch3) and (Ch3, Ch2). The combination did not involve the three channels as one vector.

In [13] Z. Ibrahim presented a steganalysis model to detect the presence of secret data in RGB color images. Statistical texture features and machine learning techniques are used. Features of an RGB image analyzed as a composite unit, also analyzing individual color channels and dual combinations of the channels. The feature set used in this work consists of 26 features per channel, which involves the Gray Level Co-Occurrence Matrix (GLCM) features of contrast, correlation, homogeneity and energy, calculated for 2-bit, 3-bit half-bytes and full bytes fragments of individual channels, skewness of full bytes and half-bytes, Entropy of full bytes and half-bytes, and also statistical features. The features applied to single channels, and the single channel features merged into dual and three-channel image feature sets. The Support Vector Machine (SVM) algorithm is the machine learning binary classifier that selected for this work .also datasets created from the clean images datasets, which were involved with hidden data using 2LSB and 4LSB stenography method.

3. PROPOSED SYSTEM

The method used to detect hidden data in images depends on the extraction of certain characteristics of the images to determine whether they contain secret data or not. Then classify that characteristics to determine the extent to which these images include hidden data. And the back propagation neural network BPNN used as a classifier to classify these properties.

A. Structure of the Proposed System

In this study, multiple methods used for extracting characteristics from images to use in the discovery of hidden data. They all shared in the same general structure with tiny differences. For instance, two methods use DFT, and the other two use DCT. Fig. 1 shows the general structure of the proposed system. The following sections illustrate the methods.

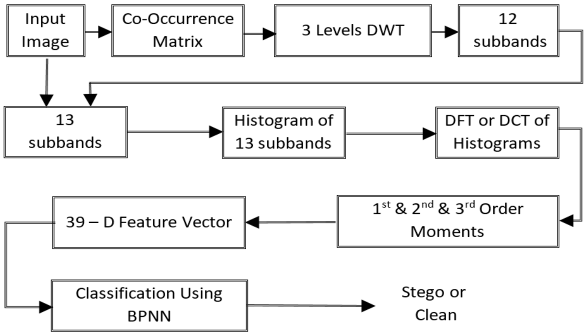

Fig. 1. The general structure of the proposed system

1- Structure of DFT

When inserting the image into the system, it is applied to three levels of DWT using the Haar filter. For each level 4 subbands, the total is 12 subbands, and the original image is added it, to be 13 subbands. After that the histogram calculated for each subband, then DFT applied to each histogram after that apply the equations of first three order of the seven-moment equations. The vector result is 39 elements. Sends to the classified BPNN to determine if the image is clean or contains a hidden.

2- Structure of CoDFT

In this system, it has the same steps as in the (DFT) system except that before inserting the image to the system is begin, the co-occurrence matrix taken for the image and then passed to the system.

3- Structure of DCT

In this system, it has the same steps as in the (DFT) system except that instead of the (DFT) it uses (DCT).

4- Structure of CoDCT

In this system, it has the same steps as in the (DCT) system except that the co-occurrence matrix for the image is taken, then the rest of the system going on.

B. Feature Extraction

The following sections discuss the concepts used to extract properties from images to determine whether they contain hidden data.

1- Data Set

Every steganographic algorithm has it own characteristics, features, and disadvantages. the method of working varies from one algorithm to another. In information hiding algorithms, it is always intended not to show deformation in the built-in cover.

The distortions are not visible to the human eye, The best way to accomplish that by taking a wide variety of cover images that do not include hidden data to get the most natural patterns to distribute the colors of the image expected to repeat in natural images. as well as a variety of embedded cover images that contain hidden data to obtain patterns of distortions by including hidden data, then draw certain characteristics of these images to distinguish them using artificial neural networks, as the neural networks can distinguish patterns that appear to be intangible.

That's hard to do is the vast amount of images available on the Internet (the medium where such hidden messages exchanged). Since the number of image data is large, and the diversity and nature of the images are very large, the diversity of natural color distribution patterns is also enormous, So, it is very difficult to determine the pattern of data distribution in images whether the distribution pattern is normal (that is, the image is clean and has not modified), or that the distribution pattern is similar to the data distribution in the embedded cover (i.e., the image contains hidden data).

The challenge is how to find a mechanism to extract certain characteristics that can distinguish natural patterns of data distribution from unnatural patterns. Methods of hiding information are many and varied, so it is difficult for the steganography analyzer to attack all the algorithms and methods of concealment common at the same time, the researcher in this area must determine the general specifications of the method of concealment that will attack.

From this point of view, it suggested in this part of the research that the system is trained and tested on a method of concealment of acceptable specifications that mimics the effect of most of the most common types of hiding. So suppose the following:

- Non-pressed images were selected.
- The selected images are varied in their content patterns and are statistically independent.
- There is no prior information on the statistical characteristics of pixels of the images that can use in the detection process, such as a particular statistical histogram.
- All cells are available for concealment, meaning that the transmitter not restricted by hiding in specific areas of the image.
- The stenography algorithm used is the Least Significant Bit (LSB).

2- Co-Occurrence Matrix

Co-Occurrence Matrix (CM) Symmetry Matrix The image of the adjacent pixels examined. This process calculates the number of times a sequence of two specific color values occurs in the entire image space. It creates a 256x256 synchronous occurrence matrix. Each element in this matrix represents the number of times of two color values. The first value is equal to the row directory value for that element, the value of the column directory for the same item. For example, if CM (85, 83) = 62 means that the value of the item in row 85 and column 83 of the CM is 62, this means that the number of times the value 85 is received immediately before the value 83 is 62 times in full Image space. The result is a 256 x 256 matrix with each element representing the number of times the row directory is synchronized with the column directory for that element since the row directory is directly in front of the column directory[14].

It is important to note that in the case of clean images, the high values of Repetition are concentrated in the main diameter of and around the co-occurrence matrix because the values of adjacent images cells are equal or very close to each other in most areas of the image. But hiding data inside the image dissipates this harmony, between the adjacent points in the image, and this is evident when comparing the co-occurrence matrix of the cover with the Co-occurrence matrix of the same image without hidden data, as we see the breadth of the area where the high-frequency value centered around the main diameter of the matrix.

3- Frequency Domain

In this section, some concepts and illustrations of DWT, DFT, and DCT will be presented.

- Discrete Wavelet Transform (DWT) is a general transform, and strong has spread widely in recent years and succeeded in using it in many fields, especially in the image field. Summarize the main idea in the work of transform the wavelet by dividing the image into four parts (LL1,LH1,HL1,HH1) where (LL1) the low frequency part represents the rest of the parts represent the contents of the high frequency, Split the part(LL1) into four other parts and so on. The reason for using this transform is an advantage in obtaining a miniature model of the original image [15]. Owing to the decorrelation capability of discrete wavelet transform (DWT), the coefficients of different subbands at the same level are kind of independent to each other. Therefore, the features generated from different wavelet subbands at the same level are kind of independent to each other. This property is desirable for steganalysis [16]. The division in this paper has adopted to three levels with Haar filter. Haar Wavelet is one of the oldest and simplest wavelet [17].
- Discrete Fourier Transform (DFT) is the process of converting the signal from the time domain to the frequency domain. So that it carries the discrete signal of value and phase, Fourier analysis is the signal process to find their reality and be the difference between the (sin) and (cos) Angle of 90 degrees And also the same angle between real and imaginary. In the frequency domain, the input must be a sine function it gives value and phase. Which returns the signal to the original is Fourier series and Fourier transform. In the Fourier domain image, represent every point a specific frequency included in the spatial domain image. Fourier Transform utilized in many usages, like image processing, image filtering, and image pressure.
- Discrete Cosine Transform (DCT) This transform is very useful to reasons effectiveness and flexibility, and it applied to samples of the signal and its characteristics that the image fragmented into two-dimensional sections [4] used this transform in this paper because of its nature into dividing the image into a set of parts.

4- *Moments*

The moment is one of the first methods adopted to achieve the constant discrimination of two-dimensional model images. It also

based on the method of algebra using a non-linear equation of the values that represent algebraic moments, a property required for stability when translating the image, modify the size (zooming) and rotation, translation, and scaling Values are the best measure for identifying characters, and digital images [16].
The seven moments considered the constant factors of any image as it does not change. And is not affected when the rotation, translation, and the scaling. And this type of moment better suited different methods of discrimination because of their fixed properties[17][18].

5- *Classification Using BPNN*

The backpropagation neural network (BPNN) system used in the proposed system for decision-making to a classification of the image to clean or Stego. By feeding the 39 properties previously extracted as mentioned in the previous sections. The cell target is one element with two values zero means (clean) or one means (Stego).
The input layer consists of 39 neurons that receive the extracted properties, while two hidden layers, the first containing 60 neurons, the second containing 30 neurons, and the transfer function used in them are Logsig. These values determined for the number of neurons and the transfer function based on the principle of experiment and error. The output layer consisted of a single neuron and used the function pureline as a transfer function. As the goals either zero means clean or one and mean Stego.
The network is trained using the number of training pairs (input and target) and then testing the network using test pairs. After completing the training process, weights and parameters of the trained network stored in a file for later use to estimate the extent to which images contain hidden data.

4. EXPERIMENTAL RESULTS

The system implemented using Matlab R2011a. For testing the proposed, a number of uncompressed gray images with various content used. The images were collected randomly and were not categorized, sorted or modified. The collection contained 110 cover images (no hidden data). 110 images of an embedded cover (include secret data), data are hidden at varying rates 1 bit per pixel (bpp), 0.1 bpp, 0.2 bpp, and 0.5 bpp. a separate network is trained for each percentage of hiding, as well as for each verity of the methods mentioned in introduction section.
Thus the group of images was randomly assigned to a training group of 70% of the group of images and a 30% test group of the remaining images. The total number of images for the training set for each image covered and the embedded cover is 77 for the cover images and 77 for the embedded cover images. The number of images for the test set for each of the images covers, and embedded cover images, 33 cover images, and 33 embedded cover images.

A. Detection Rate

Is the percentage obtained for the correct results is dependent on the true positive, true negative, false positive, and false negative obtained as shown in the following equation [19].

$$\det ection\_rate = \frac{TP+TN}{TP+TN+FP+FN}\times 100\% \qquad (1)$$

After training the hidden detection system by different data hiding percentages (0.1 bpp, 0.2 bpp, 0.5 bpp, and 1bpp) using the training data from the dataset illustrated above in this section, the system tested using the test data (which included 33 cover images and the same embedded cover images) from the same dataset. The test results based on the method used, as illustrated in Table I.

Table 1. Results Based on the Used Method

Method	Hiding Ratio	TP	TN	FP	FN	Detection Rate
DFT	0.1bpp	27	20	6	13	71.2121%
	0.2bpp	22	19	11	14	62.1212%
	0.5bpp	30	21	3	12	77.2727%
	1bpp	31	23	2	10	81.8182%
CoDFT	0.1bpp	21	29	12	4	75.7576%
	0.2bpp	29	24	4	9	80.3030%
	0.5bpp	27	27	6	6	81.8182%
	1bpp	30	20	3	13	75.7576%
DCT	0.1bpp	15	29	18	4	66.6667%
	0.2bpp	17	30	16	3	71.2121%
	0.5bpp	28	12	5	21	60.6061%
	1bpp	15	29	18	4	66.6667%
CoDCT	0.1bpp	28	20	5	13	72.7273%
	0.2bpp	30	21	3	12	77.2727%
	0.5bpp	24	29	9	4	80.3030%
	1bpp	16	30	17	3	69.6970%

B. Discussion of the Obtained Results

In general, the results obtained shown that the data embedding rate do not influence the detection rates significantly. After adding co-occurrence matrix to the DFT, better results obtained in all hidden data sizes except In the case of 1bpp, the result was better without the use of co-occurrence matrix. But the rest of the results were all the better with the presence of the co-occurrence matrix either for the addition of co-occurrence matrix to DCT has obtained better results in all cases, with all the hidden data sizes used in this paper. Fig. 2 shows a bar chart that illustrates the detection rates of the proposed system grouped by embedding ratio, where fig. 3 views the detection rates of the proposed system grouped by steganalysis method.

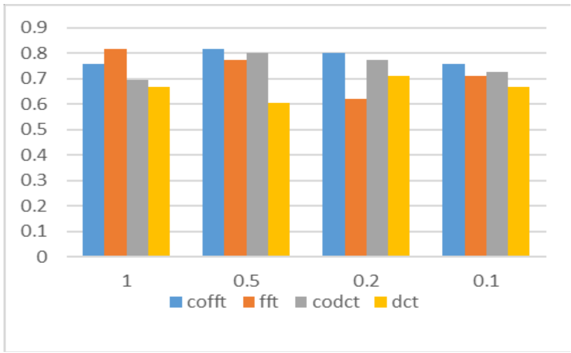

Fig. 2. Results of proposed system grouped by embedding ratio

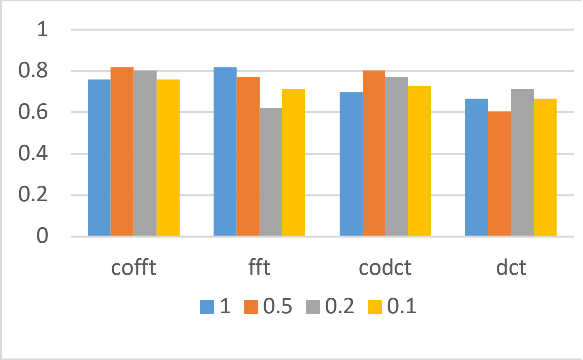

Fig. 3. Results of proposed system grouped by steganalysis method.

C. Comparison with Previous Works

When the comparison with the results of previous researches, they used the same method that used in this paper, showing that the results obtained in this paper are better than the results obtained from previous research. Especially with the addition of the co-occurrence matrix to the proposed structure, the results had become better.

Table 2. Results Based on the Used Method

Steganalysis Method	Embedding Rate = 1 bpp	Embedding Rate = 0.5 bpp	Embedding Rate = 0.2 bpp
18-D DWT features [13]	61.67 %	60 %	60 %
39-D DWT features [14]	60 %	60 %	63.33 %
78-D DWT features [12]	46.67 %	53.33 %	51.67 %
Proposed CoDFT	75.76 %	81.82 %	80.3 %
Proposed DFT	81.82 %	77.27 %	62.12 %
Proposed CoDCT	69.7 %	80.3 %	77.27 %
Proposed DCT	66.67 %	60.61 %	71.21 %

5. CONCLUSIONS

The regularity of the relationship between adjacent image cells in most picture areas provides the appropriate ground for constructing a detection system based on the nature of this relationship to determine whether the image is a cover or Stego-cover. Depending on the relationship between the adjacent image points, using the co-occurrence matrix, enabled the steganalysis to detect the hidden.

The diversity of large data within the supplied database occur Conflicts and inconsistencies, the existence of these conflicting and abnormal data confuse the work of the detection system and make the arrival of the situation of stability difficult.

The relationship between system performance and the hidden ratio is an inverse relationship in CoDFT, CoDCT, and DCT. The lower the percentage of hidden message, be more efficient the system. However, the relationship between system performance and the hidden ratio is a positive relationship in DFT, as the greater the percentage of hidden message, be more efficient the system.

REFERENCES

[1] G. R. Suryawanshi and S. n Mali, “Universal Steganalysis Using IQM and Multiclass Discriminator for Digital Images,” in *Signal Processing, Communication, Power and Embedded System (SCOPES)*, 2016, pp. 877–881.

[2] S. M. Badr and A. H. Khalil, “A Review on Steganalysis Techniques : From Image Format Point of View,” *Int. J. Comput. Appl.*, vol. 102, no. 4, pp. 11–19, 2014.

[3] S. O. Hasson and F. M. Khalifa, “Steganalysis Using KL Transform and Radial Basis Neural Network,” *Raf. J. Comp. Math’s.*, vol. 9, no. 1, pp. 47–58, 2012.

[4] M. Bachrach and F. Y. Shih, “Image steganography and steganalysis,” *Wiley Interdiscip. Rev. Comput. Stat.*, vol. 3, no. 3, pp. 251–259, 2011.

[5] J. Davidson and C. Bergman, “An Artificial Neural Network for Wavelet Steganalysis,” *Final Rep. to Midwest Forensics Resource. Cent.*, pp. 1–23, 2005.

[6] V. P. Venkatesan, “Steganalysis Using Colour Model Conversion,” *SIPIJ*, vol. 2, no. 4, pp. 201–211, 2011.

[7] R. Gong and H. Wang, “Steganalysis for GIF images based on colors-gradient co-occurrence matrix,” *Opt. Commun.*, vol. 285, no. 24, pp. 4961–4965, 2012.

[8] A. Aljarf, S. Amin, J. Filippas, and J. Shuttelworth, “Develop a Detection System for Grey and ColourStego Images,” *Int. J. Model. Optim.*, vol. 3, no. 5, pp. 3–6, 2013.

[9] J. Zeng, S. Member, S. Tan, S. Member, B. Li, and S. Member, “Large-scale JPEG image steganalysis using hybrid,” vol. 6013, no. c, pp. 1–15, 2017.

[10] M. Kaur and G. Kaur, “Review of Various Steganalysis Techniques,” *Int. J. Comput. Sci. Inf. Technol.*, vol. 5, no. 2, pp. 1744–1747, 2014.

[11] C. G. Eichkitz, J. Davies, J. Amtmann, and M. G. Schreilechner, “Grey level co-occurrence matrix and its application to seismic data,” *First Break*, vol. 33, no. 3, pp. 71–77, 2015.

[12] C. Di Ruberto, G. Fodde, and L. Putzu, “On Different Colour Spaces for Medical Colour Image Classification,” in *International Conference on Computer Analysis of Images and Patterns*, pp. 477–488, 2015.

[13] Z. I. Rasool, “The Detection of Data Hiding in RGB Images Using Statistical Steganalysis,” M. Sc. Thesis, Middle East University, 2017.

[14] B. S. V, A. Unnikrishnan, and K. Balakrishnan, “Grey Level Co-occurrence Matrices : Generalisation and Some New Features,” *Int. J. Comput. Sci. Eng. Inf. Technol.*, vol. 2, no. 2, pp. 151–157, 2012.

[15] P. Balakrishnan, “Design and Implementation of Lifting Based Daubechies Wavelet Transform Using Algebraic Integers,” M. Sc. Thesis, University of Saskatchewan, 2013.

[16] Shi, Yun Q., Guorong Xuan, Dekun Zou, Jianjiong Gao, Chengyun Yang, Zhenping Zhang, Peiqi Chai, Wen Chen, and Chunhua Chen. “Image steganalysis based on moments of characteristic functions using wavelet decomposition, prediction-error image, and neural network,” *IEEE Int. Conf. Multimedia. Expo, ICME*, pp. 269–272, *2005.*

[17] Xuan, GR & Shi, Y.Q. & Gao, JJ & Zou, D & Yang, CY &

Zhang, ZP & Chai, PQ & Chen, CH & Chen, Wen. "Steganalysis based on multiple features formed by statistical moments of wavelet characteristic functions." 7th International Workshop on Information Hiding, Vol. 3727, pp. 262-277, 2005.

[18] Shi, Yun Q., Guorong Xuan, Chengyun Yang, Jianjiong Gao, Zhenping Zhang, Peiqi Chai, Dekun Zou, Chunhua Chen, and Wen Chen. "Effective Steganalysis Based on Statistical Moments of Wavelet Characteristic Function," in *IEEE International Conference on Information Technology: Coding and Computing*, vol. 1, pp. 768–773, 2005.

[19] Desai, Madhavi B., and S. V. Patel. "Performance analysis of image steganalysis against message size, message type and classification methods." In IEEE International Conference on Advances in Electronics, Communication and Computer Technology (ICAECCT), pp. 295-302. IEEE, 2016.