Computational Analysis of Arabic Cursive Steganography using Complex Edge Detection Techniques

Anwar H. Ibrahim[1], Abdulrahman S. Alturki[2]
College of Engineering, Qassim University
Mulaidah, Qassim Province
Saudi Arabia

***Abstract*—Arabic language contains a multiple set of features which complete the process of embedding and extracting text from the compressed image. In specific, the Arabic language covers numerous textual styles and shapes of the Arabic letter. This paper investigated Arabic cursive steganography using complex edge detection techniques via compressed image, which comprises several characteristics (short, medium and Long sentence) as per the research interest. Sample of images from the Berkeley Segmentation Database (BSD) was utilized and compressed with a diverse number of bits per pixel through Least Significant Bit (LSB) technology. The method presented in this paper was evaluated based on five complex edge detectors (Roberts, Prewitt, Sobel, LoG, and Canny) via MATLAB. Canny edge detector has been demonstrated to be the most excellent solution when it is vital to perform superior edge discovery over-compressed image with little several facts, but Sobel appears to be better in term of the execution time for Long sentence contents.**

Keywords*—Arabic language; Berkeley Segmentation Database (BSD); Least Significant Bit (LSB); Roberts; Prewitt; Sobel; LoG; Canny

I. Introduction

Protected of correspondence information between two nodes through a communication system ought to be secured from attack, consequently, numerous ways are utilized for that reason. Data covering up is utilized for forestalling an interloper to recognize them. Steganography is a method used to shroud the data and send them to the sender with changed over an arrangement to secure the data [1]. Another method provides high security to the data is the cryptography. It keeps data over the organization through changing over the plaintext into figure text. A few kinds of cryptography are utilized which are symmetric, topsy-turvy, and hashing. Cryptography calculation utilizes a similar key for encryption and unscrambling measures is called symmetric cryptography, while unbalanced cryptography utilizes various keys for encryption and decoding.

The transmission of a huge amount of information over the channel in a communications network involves high protection to secure the information. Consequently, steganography has a crucial function in communication to encapsulate such data throughout the edge and cover of an image. Steganography is practised by using those wishing to deliver a mystery message or code through the image. While many valid methods make use of the steganography, such malware builders have additionally been located to use steganography to obscure the transmission of malicious code. Steganographic methods categorized into two classes: transform domain names and spatial methods [2]. Virtual Image for Steganography is one frequently [3]; which required two documents: The message to be embedded into the images for secretly hidden [4]. Steganography based data protection is crucial for confidential facts transfer. There are 3 fundamental requirements within the subject of digital steganography, each significant of mystery information is represented by the way of 8 bits and those bits are embedded inside the edge of the photo once creating the arithmetic processes on it. The first fundamental condition is capacity, which depends on the number of secret bits to be embedded in each cover pixel. The second constraint is robustness that avoids hidden information from attack. The third obligation is imperceptibility, typically intended by peak signal to noise ratio (SNR). Thus, Steganography technology is truly important in terms of information destiny of internet protection and privacy on open systems inclusive of the network which considered respectable when the faintness is high during secret data transmission while needing communication robustness [5]. Most of the existing methods using the Least Significant Bit (LSB) due to the redundant bits on the cover of the images embeds in the spatial area of the image with less effective in which it occurring clear misrepresentation [6,7].

II. Background of Steganography

As stated formerly, photographs are taken into consideration because of the maximum famous record formats used in steganography. They are acknowledged for constituting a non-causal medium, because of the possibility to get entry to any pixel of the photograph at random. Further, the hidden data should continue to be invisible to the attention. Fig. 1 represents the general data protection scheme Classification tree.

Steganography is another way of having messages secured during data communication. The end goal of steganography and cryptography is the same but they have different methods. Steganography does not change data or message format and keeps its actual data present while cryptography keeps the data secret by converting it into an unreadable form. The drawback

of the cryptographic approach lies in the existence of original data as the original data was encrypted. Steganography techniques, therefore, provide additive protection to cryptographic techniques. This offers an additional layer of protection for the message during data communication, with the combination of both.

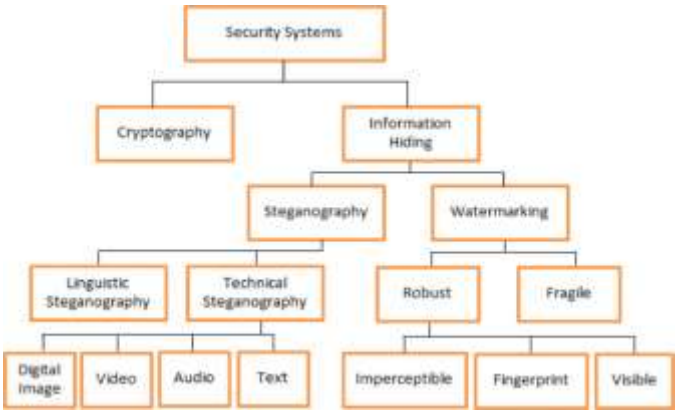

Fig. 1. Classification Tree of Security Systems [8].

III. Steganography Features

A. Why Steganography is Important?

Nowadays, Steganography can be utilized to cover up hidden information interior to other files so that the parties expecting to induce the message indeed knows a mystery message exists. steganography gets to be the foremost basic approach utilized to secure the information. The word steganography implies, hide the secret information just like e-content or advanced arrange. It points to conceal the mystery information eventually between two parties and make it not visual to the third party and without any doubts around the existing of any covered up data. There are a few sorts of steganography have been isolated into two mediums, which are advanced steganography and normal dialect steganography. Computerized steganography is the craftsmanship that bargains with the computerized medium, for illustration, picture, video, and sound, whereas characteristic dialect steganography bargains with the content records. Indeed even though computerized steganography has the most considerations by the analysts, in any case, the content is the foremost basic information that has to be secured since most of the documentation will be within the content such as sending basic data or doling out pressing appointments [9,10]. Also, steganography in the natural language is divided into two groups, which are linguistic steganography and steganographic text. Linguistic steganography is about the text (a secret message) concealed in a text medium [8]. In the meantime, auto-steganography adjusts the document format or a specific character, without altering the context of the sentences [11, 12].

Hiding the data involves certain strategies using the natural language steganography. The sort has its techniques which are, word-rule-based and feature-based techniques used by the researchers in text steganography [13]. Meanwhile, linguistic steganography uses five techniques, such as synonymous substitution, syntactic substitution, semantic substitution, PCFG, and hybrid technique.

B. Steganography Features based Technique

So far, numbers of image steganography methods have been implemented, the simplest approach implemented is the LSB substitution technique. The least important bits of the picture pixel are used in this technique for embedding hidden message bits [14,15].

The feature-based approach works, for example, with the shape or style of the text, by modifying the size or type of font. This strategy will make readers believe that no improvements are made in Text so that the reader cannot notice the hidden message embedded in the cover [16].

IV. Embedding and Extraction Techniques

A Steganography embedding and extraction technique refer to all items with redundancy in the data. People frequently transfer digital images through email and other Internet communication and JPEG is one of the most popular image formats. Also, steganography systems seem more appropriate for the JPEG format because the systems run in a transformed space and are not affected by visual attacks [8].

An image's edge representation greatly decreases the amount of data to be processed, but it preserves important knowledge about the shapes of the objects in the picture. This description of an image is easily implemented in a large number of object recognition algorithms used in computer vision along with other applications for image processing. The edge detection technique's main property is its ability to determine the exact edge line with reasonable orientation, as well as more literature on edge detection has been available in the last three decades. On the other hand, the efficiency of the edge detection techniques is not yet measured by any typical performance index. The efficiency of an edge detection technique is often judged individually and independently based on its application. The literature includes several edge detection techniques for image segmentation. This section looks at the most widely used discontinuity-based edge detection techniques. These are Roberts edge detection methods, Sobel Edge detection, Prewitt edge detection, Kirsh edge detection, Robinson edge detection, Marr-Hildreth edge detection, LoG edge detection and Canny Edge detection [17].

A. Roberts Edge Detection

Lawrence Roberts (1965) implements Roberts Edge Detection. It performs a simple, easy to calculate, 2-D measurement of the spatial gradient on an image. This approach emphasizes high-spatial-frequency regions that often correspond to edges. The operator input is a grayscale image the same as the output is the most common use for this technique, pixel values at each point in the output reflect the approximate complete magnitude of the input image's spatial gradient at that point [18]. The Roberts Edge filter is used to detect edges that are based on sequentially applying a horizontal and vertical filter as shown in table A and B. Both filters refer to the image and are summed up to create the final picture.

A.Horizontal Filter

0	1
1	0

B. Vertical Filter

1	0
0	1

B. Prewitt Edge Detection

Prewitt in (1970) proposed by Rafael C for edge detection technique. It was found that as a correct way to estimate the magnitude and orientation of the edge. Although different gradient edge detection requires a time-consuming calculation to estimate the direction from the magnitudes in the x and y directions, the compass edge detection obtains the direction directly from the kernel with a high grade of reacting. This gradient-based edge detector is estimated for eight directions in the 3x3 area. All 8 convolution masks are calculated. A complication mask is then selected, i.e. for the largest module [19].

A.Horizontal Magnitudes

-1	-1	-1
0	0	0
1	1	1

B. Vertical Magnitudes

-1	0	1
-1	0	1
-1	0	1

C. Sobel Edge Detection

The Sobel method introduced by Rafael C (1970) for the segmentation of the image finds the edges using the Sobel approximation to the derivative. It precedes the edges at the points where the gradient is the highest. The Sobel technique performs a 2-D spatial gradient quantity on the image, thus highlighting regions with a high spatial frequency corresponding to the edges. In general, it is used to find the estimated absolute gradient magnitude for each gradient [18].

A.Horizontal Magnitudes

-1	-2	-1
0	0	0
1	2	1

B. Vertical Magnitudes

-1	0	-1
-2	0	2
-1	0	1

D. LoG Edge Detection

The Laplacian of Gaussian (LoG) was introduced by Marr (1982) for edge detection. Laplacian filters are derivative filters that are used to detect areas of rapid change (edges) in images as shown at equation (1) for the relation of the second derivative of image *f(x,y)* [20].

$$\nabla^2 f = \frac{\partial^2 f}{\partial x^2} + \frac{\partial^2 f}{\partial y^2} \quad (1)$$

Since the derivative filters are very sensitive to noise, it is common to smooth the image using a Gaussian filter before applying the Laplacian filter. Subsequently, the operator of Laplace can detect both edges and noise (isolated, out-of-range), it may be desirable first to smooth the image with a Gaussian kernel of width.

E. Canny Edge Detection

The Canny edge detector is an operator of the edge detection, using a multi-stage algorithm to detect a wide range of edges in images. It was founded in 1986, by John F. Canny. Canny also developed a computational edge detection theory which explains why the technique works. In industry one of the popular edge detection techniques is the Canny edge detection technique. It was first created by John Canny for his Master's thesis at MIT in 1983, and it still outperforms many of the newer algorithms that have been developed. To find the edges by separating the noise from the image before finding the edges of the image, Canny is a very important method [17].

V. A Proposed Method for Embedding and Extraction Steganography

The proposed method of image steganography intends to improve/increase the cover image's hiding capacity. The suggested approach uses the inclusion of the edge region in the cover picture to add more hidden information than embedding it into the non-edge region. The method of embedding and extraction in the proposed work is Widespread introduced in two steps. Transmitter and receiver with high secure user name and password. Fig. 2 shows the steps of embedded and extracted Arabic text steganography.

An important aspect of the techniques used in this thesis is that it used to embed a text in colour images. Fig. 2 shows the button to select an algorithm to be considered from six types (Log, Robert, Prewitt, Canny, Demirel, and Sobel) to perform the proposed method. The user has an option to choose only one algorithm to embed the text as shown in Fig. 2.

The method of modification of the Least Significant Bit (LSB) is used very effectively in the Image Steganography technique. To enhance its wide-ranging application, this research paper proposes that, as a first step, this method can also be applied to images that have undergone edge detection techniques the reason why the edge detected image is different from the original image so that any edge detection changes can be made.

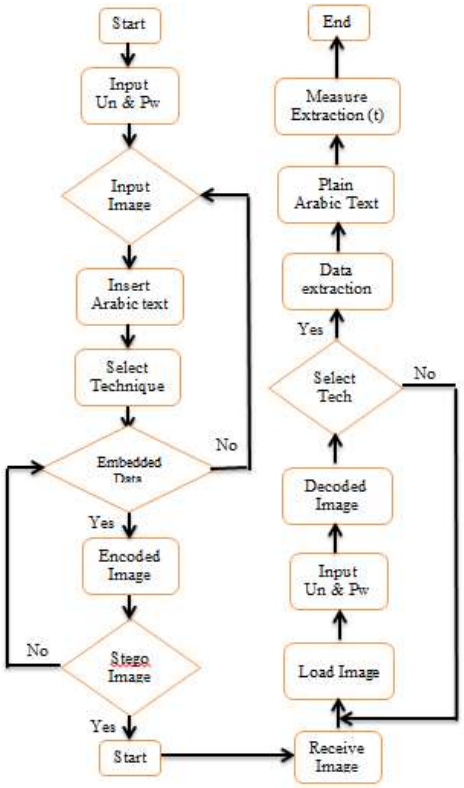

Fig. 2. State Transition Diagram of Proposed Steganography.

A. The Unicode Standard

Unicode is a universal standard that was adopted for the production, encoding, and handling of digital texts represented in most of the writing systems in the world from 1987 until now [21]. The Unicode standard, in other words, is an encoding scheme designed to facilitate the worldwide display, processing and exchange of texts with different languages and technical discipline.

B. Arabic Text Hiding Criteria

When programmers build a text hiding algorithm there are many things to remember. In recently implemented algorithms, however, the fundamental requirements can be easily found: invisibility, embedding power, robustness, and security [22]. For an active or passive warden, respectively, the contact medium through which the stego-image is being transmitted can be noisy or noiseless.

C. Arabic Text Embedding and Extraction

The information stream of image format (MPEG, JPG and SVG) were mostly made out of head data, image encoded information on vector stream utilizing movement remuneration forecast method with a least significant bit (LSB) created movement vector information stream. The design-based strategies include changing a few highlights of the spread content of text embedding, for example, text dimension, style, shading, and so forth that could be modified to cover mystery image. In the extraction process, the inverse method should be applied to extract the data we less time according to the image format and capacity.

D. Algorithm Selection

A significant part of the procedures utilized in this theory is that it used to insert a book in shading pictures. Fig. 2 shows the catch to choose calculation to be considered from six sorts (Robert, Prewitt, Canny, Log, and Sobel) to play out the proposed technique. The client has an alternative to pick just a single calculation to install the content as appeared in Fig. 2.

VI. Results and Discussion

The research proposed is designing robust algorithms to perform the Results:

Increase robustness by embedding random bit in the edge of the image, employing value shift technique based Matlab algorithms. The concept is only Embedding bits in the consecutive pixels of the samples in the selected area.

Table I displays the steganography overall description techniques and provides a clear understanding that each technique has its advantages and inconveniences. Each is unique to the application and the program requirement justifies the use of such a system with given parameters. Sobel is one of the most successful techniques for the systems requiring fast computation without having to maintain data.

Fig. 3 represented the level of the embedding and extraction time of Arabic text steganography which are limit intangibility, accessibility, and reading time.

Fig. 4 shows the inexact implanting time and the all-out limit character for every calculation through three configurations; it was discovered that the best calculation for stage installing is finished by the Canny method.

The primary edge assessment was limit according to the image format utilization, the representation capacity measured based on three image format, based on the classification, accessibility, and capacity that utilized the total measure.

TABLE I. Overall Description Techniques of Steganography

Parameters	Pewit	Sobel	Canny	Roberts	LoG
Comput-tional	Comple x	Simple	Complex	simple	Complex
Signal to Noise ratio	Low	Low	High	High	Low
Texture based image	Less efficient	High efficien t	Less efficient	Less efficient	High efficient
Embeddin g time	less time	efficien t time	time-consumin g	time-consumin g	efficient time
Extraction time	less time	efficien t time	time-consumin g	time-consumin g	time-consumin g
Security	more	less	more	less	more
Capacity	more	less	more	more	less

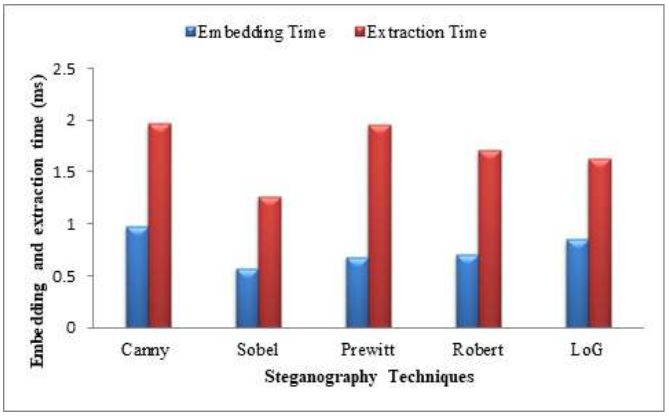

Fig. 3. Embedding and Extraction Time.

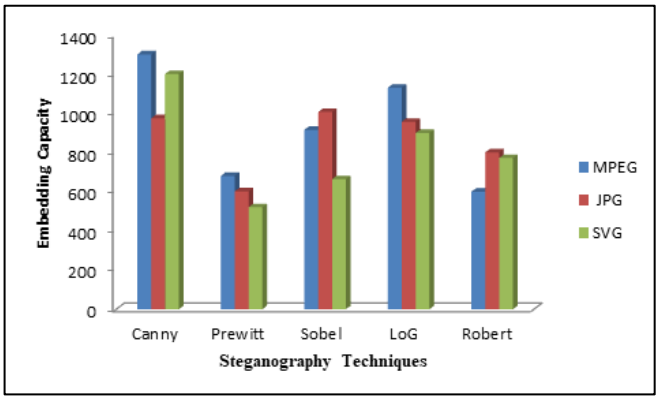

Fig. 4. Embedding Capacity.

VII. CONCLUSION

The proposed strategy applies the edge discovery method on the spread picture and disorderly guide. We utilized the edge location method with the end goal that Sobel channel, it is utilized to give various pieces utilized in installing. Likewise, we utilized tent guide, it gives the area of pixels which used to inserting pieces. The trials and result directed to affirm that stego-picture inserts the two mystery bits if pixel present edges or installs the one mystery bit if pixel, not the current edge. We utilized the arrangement of the measures to discover the proportion of clamour between pictures. This contextual investigation presents an examination of existing content concealing methods, particularly on those concentrated on adjusting the basic attributes of advanced instant message for Arabic text. The results outlined a scope of crucial rules, applications, and assaults covering the content concealing territory to clarify the current embedding and extraction time challenges in the image steganography. Additionally, the study concludes the three significant evaluation process (Extraction time, Embedding time and effect of the image format) of Arabic text concealing procedures dependent on the best way to deal with spread instant messages to decode the mystery bits, in particular, the maximum capacity with less time for embedding and extraction time. Based on the critical condition for the best sketched out the restrictions and qualities of every classification to show their effectiveness in different image format. Also, we assessed the as of late proposed approaches concerning the key measures to feature their advantages and disadvantages. Finally, we have suggested some of the rules and bearings that legitimacy further consideration in future works.

REFERENCES

[1] Hassanain Raheem Kareem, Hadi Hussein Madhi, Keyan Abdul-Aziz Mutlaq. Hiding encrypted text in image steganography. Periodicals of Engineering and Natural Sciences. Vol. 8, No. 2, June 2020, pp.703-707.

[2] A. Cheddad, J. Condell, K. Curran, P. Mc Kevitt, “Digital image steganography: Survey and analysis of current methods”, Signal Processing, Volume 90, Issue 3, March 2010, Pages 727-752.

[3] A. Cheddad, J. Condell, K. Curran, and P. McKevitt, "Digital image steganography: Survey and analysis of current methods", Signal Processing, vol. 90, no. 3, pp. 727-752, 2010.

[4] B. Li, J. He, J. Huang, and Y. Q. Shi, "A survey on image steganography and steganalysis", Journal of Information Hiding and Multimedia Signal Processing, vol. 2, no. 2, pp. 2073-4212, 2011.

[5] Kehui Sun, “Chaotic secure communication: principles and technologies,” Berlin Boston De Gruyter, 2016.

[6] Ramadhan J. Mstafa and Khaled ElleithyKhaled Elleithy, “A Novel Video Steganography Algorithm in the Wavelet Domain Based on the KLT Tracking Algorithm and BCH Codes. 015 IEEE Long Island Systems, Applications, and Technology Conference At: NYC, May 2015.

[7] G. Sugandhi and C. P. Subha . Efficient steganography using least significant bit and encryption technique . 2016 10th International Conference on Intelligent Systems and Control (ISCO). 7-8 Jan. 2016.Wavelet Domain Based on the KLT Tracking Algorithm and BCH Codes”, 2015.

[8] Karrar Abdallah Mohammed, Int. Journal of Computer Science & Mobile Computing, Vol.7 Issue.10, October- 2018, pg. 25-32.

[9] R. Din and S. Utama, “Critical Review of Verification and Validation Process in Feature-Based Method Steganography,” in Int. Conf. E-Commerce, 2017, pp. 15-19.

[10] S. S. Iyer and K. Lakhtaria, “New robust and secure alphabet pairing Text Steganography Algorithm,” Int. J. Curr. Trends Eng. Res., vol. 2, no. 7, pp. 15-21, 2016.

[11] H. T. Ciptaningtyas, R. Anggoro, and M. B. A. Fadhillah, “Text Steganography on Sundanese Script using Improved Line Shift Coding,” in 2018 International Electronics Symposium on Knowledge Creation and Intelligent Computing (IES-KCIC), 2018, pp. 254-261.

[12] S. Utama, R. Din, and M. Mahmuddin, “The Performance Evaluation of Feature-Based Technique in Text Steganography,” J. Eng. Sci. Technol., vol. 12, pp. 169-180, 2017.

[13] R. Din, R. Bakar, S. Utama, J. Jasmis, and S. J. Elias, “The evaluation performance of a letter-based technique on text steganography system,” Bulletin of Electrical Engineering and Informatics, vol. 8, no. 1, pp. 291-297, 2019.

[14] Deepali Singla and Mamta Juneja. New Information Hiding Technique using Features of Image. Journal of Emerging Technologies in Web Intelligence 6(2). 237-242. 2014.

[15] Farah Qasim Ahmed Alyousuf, and Roshidi Din. Analysis review on feature-based and word-rule based techniques in text steganography. Bulletin of Electrical Engineering and Informatics.Vol. 9, No. 2, April 2020, pp. 764~770. (Main).

[16] A. Westfeld and A. Pfitzmann, “Attacks on Steganographic Systems,” Proc. Information Hiding 3rd Int’l Workshop, Springer Verlag, pp. 61–76, 1999.

[17] Muthukrishnan.R and M.Radha. International Journal of Computer Science & Information Technology (IJCSIT) Vol 3, No 6, Pp: 259 – 267. Dec 2011.

[18] Rafael C. Gonzalez, Richard E. Woods & Steven L. Eddins (2004) Digital Image Processing Using MATLAB, Pearson Education Ltd. Ltd, Singapore.

[19] Inas Jawad Kadhim, Peter James Vial and Brendan Halloran. A comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research. Neurocomputing. Volume 335, 28 March 2019, Pages 299-326.

[20] Srinivas B.L, Hemalatha and Jeevan K.A. Edge Detection Techniques for Image Segmentation. International Journal of Innovative Research in Computer and Communication Engineering. Vol. 3, Special Issue 7, October 2015.

[21] Robert Lockwood and Kevin CurranKevin Curran. Text based steganography. International Journal of Information Privacy Security and Integrity 3(2):134. January 2017.

[22] Milad Taleby Ahvanooey, Qianmu Li, Jun Hou, Ahmed Raza Rajput and Chen Yini. Modern Text Hiding, Text Steganalysis, and Applications: A Comparative Analysis. Entropy. Entropy 2019, 21, 355.