Towards Image Steganography Using Type-2 Fuzzy Logic and Edge Detection

Hala Salih Yusuf
College Of Graduate Studies
Sudan University Of Science And Technology
Khartoum, Sudan
hala_salih@hotmail.com

Hani Hagras
The Computational Intelligence Centre
School of Computer Science and Electronic Engineering
University of Essex, United Kingdom

Abstract— **Steganography is an art and a science to hide the existence of secret communication from the third party. The communication is only known to sender and receiver. For hiding messages, various types of media are used. Image steganography is the technique that uses an image to conceal information. However, image steganography face very high uncertainty levels.**

In this paper, we will present work in progress to employ image steganography using the Least-Significant-Bit (LSB) method to embed the secret message in an image cover. We will use type-2 fuzzy logic systems and edge detection techniques to increase edge pixels, and embed more secret data into the edge pixels than the non-edge pixels based on the Least Significant Bit (LSB) substitution technique. The performance of the proposed method will be evaluated by comparing both the original image and stego image using metrics like Peak Signal to Noise Ratio (PSNR), Mean Squared Error (MSE) and Histograms.

Keywords— Steganography, type-2 fuzzy logic, edge detection

I. INTRODUCTION

The aim of computer security involves protection of information and property from stealing, corruption, or natural disaster, while allowing the information and property to remain accessible and productive to its intended users [1]. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Unfortunately, it is sometimes not enough to keep the contents of a message secret and it may also be necessary to keep the existence of the message secret. The technique for solving the problem, is called steganography [2].

Steganography is an art and science which hides the existence of the secret communication, the communication is only known to both sender and receiver [3]. It is derived from the Greek word stegano which means “covered” and graphia means “writing or drawing” [4]. The main goal of steganography is that the existence of the secret message is not known [5], but in cryptography the secret message is converted into a different form. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Steganography and cryptography share a common goal, and both are closely related concepts [2]. Unfortunately, it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. The technique to solve this problem is called steganography. Fig.1 shows various disciplines of information hiding [6].

Steganography and cryptography are considered cousins in the family of spy craft. Cryptography scrambles a message so that it cannot be understood. Steganography hides the message so it cannot be seen [7].

Steganography can be applied to various objects like text, image, audio or video etc. These objects are called cover object or carrier object of the stenographic method. The secret message can also be of types like text, image, audio or video etc. These objects are called message object. After the application of a steganography method, the produced output file is called stego object.

As shown in Fig. 2, depending on the nature of carrier object, steganography can be divided into five types [8]:

- Text Steganography
- Image Steganography
- Audio Steganography
- Video Steganography
- Protocol Steganography

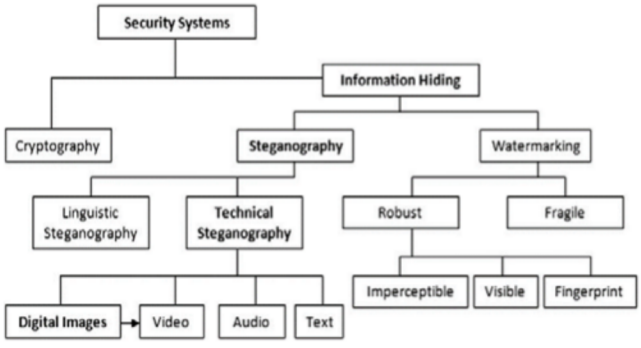

Fig. 1. shows various disciplines of information hiding [6].

The paper is organized as follows, Section II presents an overview of different image steganography approaches while Section III presents an overview of the work in progress to develop type-2 fuzzy logic and edge detection systems for image steganography.

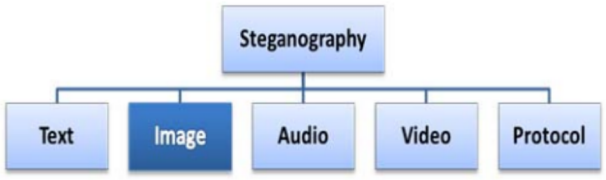

Fig. 2. Steganography Types depends on the cover object [8].

II. An Overview of Image Steganography Approaches

A. Image Steganography

As shown in Fig. 3, Image Steganographic techniques can be divided in to two groups [5]: the Spatial domain technique group and the Transform domain group. The Spatial domain technique embeds information in the intensity of the pixels directly, while the Transform domain technique embeds information in frequency domain of previously transformed image [4], [5], [9], [10].

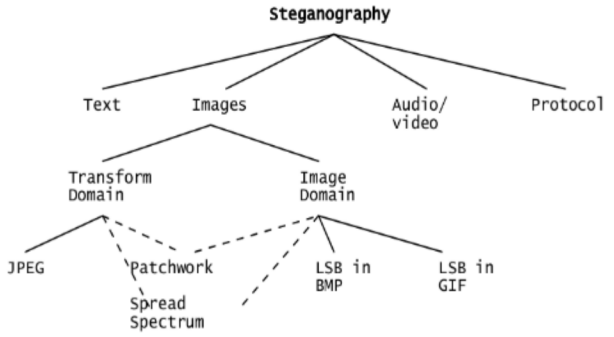

Fig. 3. Categories of image steganography [8].

In [11], Wu et al proposed a steganographic method based on Least-Significant-Bit (LSB) replacement and pixel-value differencing (PVD) method. A steganography approach based on the combination of LSB substitution mechanism and edge detection was proposed by Bai et al [9]. The cover pixels were classified by edge areas and non-edge areas. Then, pixels that belong to the edge area are used to carry more secret bits.

In [12], an evolutionary process was proposed to create a secure steganographic encoding on JPEG images. In [13], Wang et al presented a steganography where after embedding the secret message in LSB of the cover image, the pixel values of the steg-image are changed by the genetic algorithm to keep their statistical characters. The experimental results showed the proposed algorithm's effectiveness in resistance to steganalysis with better visual quality.

In [14], Kanan et al proposed a tunable visual image quality and data lossless method in spatial domain based on a genetic algorithm where the proposed technique relied on modeling the steganography problem as a search and optimization problem.

In [15], Rana et al proposed image steganography method based on kohonen neural network. In [16], El-Emam proposed three-phase intelligent technique to develop the data-hiding algorithm in colour images with imperceptibility. The results of the proposed algorithm can efficiently embed a large quantity of data, up to 12 bpp (bits per pixel), with better image quality.

Chen et al. [17] proposed a hybrid edge detection scheme combined of the fuzzy edge detector and the Canny edge detector to get more edge pixels, and embedded more secret data into the edge pixels than the non-edge pixels based on the Least-Significant-Bit (LSB) substitution scheme. In [18], Kaur et al proposed Fuzzy Logic edge detector (FLED) with the ability of detecting plenty of edge pixels, which makes good preparations for the future embedding procedure. In [19], Tseng and Leng presented a scheme combed with Kaur et al.'s fuzzy logic-based algorithm [18] .

B. Image definition

To a computer, an image is a collection of numbers that constitute various light intensities in various areas of the image. This numeric representation forms a grid and the individual points are referred to as pixels. The majority of images on the Internet consists of a rectangular map of the image's pixels (represented as bits) where each pixel is located and its color. These pixels are displayed horizontally row by row. The number of bits in a color scheme, called the bit depth, refers to the number of bits used for each pixel. The smallest bit depth in current color schemes is 8, meaning that there are 8 bits used to describe the color of each pixel. Grey scale and monochrome images use 8 bits for each pixel and are capable of displaying 256 various colours or shades of grey. Digital color images are typically stored in 24-bit files and use the RGB color model, also known as true color. All color variations for the pixels of a 24-bit image are derived from three primary colors: red, green and blue, and each primary color is represented by 8 bits [8].

C. Least Significant Bit

The Least-Significant-Bit (LSB)-based approach is a popular type of steganographic algorithms in the spatial domain [20], [21]. LSB insertion is a common, simple approach to embedding information in a cover image [22],[23]. The least significant bit (in other words, the 8 bit) of some or all of the bytes inside an image is changed to a bit of the secret message. When using a 24-bit image, a bit of each of the red, green and blue color components can be used, since they are each represented by a byte. For example a grid for 3 pixels of a 24-bit image can be as follows [8]:

```
(00101101   00011100   11011100)
(10100110   11000100   00001100)
(11010010   10101101   01100011)
```

When the number is 200, where the binary representation is 11001000, is embedded into the least significant bits of this part of the image, the resulting grid is as follows:

```
(00101101   00011101   11011100)
(10100110   11000101   00001100)
(11010010   10101100   01100011)
```

D. Human Visual System (HVS)

Image steganography takes the advantage of limited power of Human Visual System (HVS) [12]. According to research the human eye is more sensitive to changes in the brightness (luminance) of a pixel than to changes in its color (chrominance) [8].

E. Edge detection

Edge detection is a terminology in electronic vision, particularly in the areas of feature extraction, to refer to algorithms which aim at identifying points in a digital image at which the image brightness changes sharply or more formally has discontinuities [22]. The goal of edge detection is to locate the pixels in the image that correspond to the edges of the objects seen in the image [18]. Essentially, edge detection is adopted to indicate the abrupt changes in the intensity of an image and identify the current pixel, a non-edge pixel or an edge pixel.

There are many standard edge detection algorithms such as Sobel, Prewitt, Roberts, Laplacian and Canny operators [9].

III. Overview of the Work in Progress to Develop Type-2 Fuzzy Logic and Edge Detection Systems for Image Steganography

The concept of Fuzzy Logic (FL) was introduced by the founding father of the entire field Zadeh in the 1960s. Basically, Fuzzy Logic aims to mimic human-like style of thinking in the programming of computers [20]. Fuzzy logic provides the wherewithal of calculating medium values between absolute true and absolute false with resulting values ranging between 0.0 and 1.0 [24], [25] [26].

Using fuzzy logic, it is possible to calculate the degree to which an item is a member. Fuzzy logic calculates the shades of gray between black/white and true/false.

A Fuzzy Logic System (FLS) maps crisp inputs into crisp outputs[21] [27]. It contains four components which are rules, fuzzifier, inference engine, and defuzzifier. Once the rules have been established, a FLS can be viewed as a mapping from inputs to outputs and this mapping can be expressed quantitatively as $y = f(x)$ [28], [29].

The type-2 Fuzzy Logic System (FLS) (shown in Fig. 4) was firstly introduced by Lotfi Zadeh in 1975 [30], [31]. A type-2 fuzzy set is characterized by fuzzy membership functions which are themselves fuzzy [30]. A type-2 membership value (or membership grade) for each element can be any subset in [0, 1], differently a type-1 fuzzy set where the membership grade is a crisp number in [0, 1] [31], [32] [33]. The membership functions of type-2 fuzzy sets are three dimensional and include a footprint of uncertainty, it is the new third dimension of type-2 fuzzy sets and the footprint of uncertainty that gives additional degrees of freedom that make it reasonable to directly model and handle uncertainties [31]-[33]. The type-2 fuzzy sets are beneficial where it is difficult to determine the exact and precise membership functions [33].

From previous studies that have been done in fuzzy logic, edge detection and Image steganography, the strength and weakness points of each method were recognized. Based on this, a type-2 fuzzy logic based image steganography method will be employed due to its ability to handle the high level of uncertainty present in images. The type-2 fuzzy systems will be employed in conjunction with LSB substitution and edge detection, to classify cover image pixel into edge pixels and non-edge pixels.

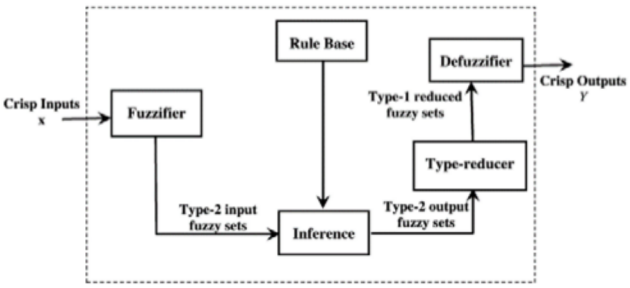

Fig. 4. Type 2 Fuzzy Logic Controller [30].

The performance of the proposed method will be tested by comparing both the original image and stego image by Peak Signal to Noise Ratio (**PSNR),** Mean Squared Error (**MSE**) and Histograms. We will use the standard images for image steganography like 'Lena','Peppers',' Baboon' and 'Mona Lisa'.

IV. Conclusions and Future Work

Image steganography is the technique that uses an image to conceal information. Steganography techniques aims to increase capacity of the converted media as well as increasing the robustness of stego object against passive and active attacks. In addition, steganography aims to increase the imperceptibility in the process of embedding a secret message into stego object. However, image steganography face very high uncertainty levels. Hence, it is important to balance these three requirements in the fields of information hiding while handling the encountered uncertainties.

The proposed system will be designed to increase capacity, robustness and complexity by using type-2 fuzzy logic systems, edge detection and LSB substitution to embedded secret message. In our current and future work, we will present the system results where the performance of the proposed system will be tested by comparing both the original image and stego image by Peak Signal to Noise Ratio (**PSNR),** Mean Squared Error (**MSE**) and Histograms. The proposed system will be designed to increase capacity, robustness and complexity by using type-2 fuzzy logic systems, edge detection and LSB substitution to embedded secret message. We will use the standard images for image steganography like 'Lena','Peppers',' Baboon' and 'Mona Lisa'.

REFERENCES

[1] A. Gadichal , "Audio Wave Steganography", International Journal of Soft Computing and Engineering (IJSCE), Vol. 1, No. 5, 2011.

[2] M. Subhedar and V. Mankar, "Current status and key issues in image steganography: A survey," Elsevier, September 2014.

[3] Xiang-Yang Luo , Dao-Shun Wang , Ping Wang and Fen-Lin Liu , "A review on blind detection for image steganography," Signal Processing - elsevier, vol. 88, no. 9, pp. 2138– 2157, April 2008.

[4] L. Marvel , C. Boncelet, and C. T. Retter , "Spread Spectrum Image Steganography", IEEE Transactions on image processing, Vol. 8, No. 8, pp. 1075-1083, August 1999.

[5] A. Ioannidou , S. Halkidis , and George Stephanides , "A Novel Technique for Image Steganography Based On a High Payload Method and Edge Detection", Expert Systems with Applications- Elsevier, Vol. 39, No. 14, pp. 11517-11524, October 2012.

[6] A. Cheddad , J. Condell , K. Curran, and P. Mc Kevitt , "Digital image steganography: Survey and analysis of current methods" Elsevier, 2010.

[7] S. Arora and S. Anand, "A Proposed Method for Image Steganography Using Edge Detection", International Journal of Emerging Technology and Advanced Engineering, Vol. 3, No. 2, February 2013.

[8] T. Morkel , J. Eloff and M. Olivier , "An Overview of Image Steganography", Information and Computer Security Architecture (ICSA) Research Group, 2005.

[9] J. Bai , C. Chang , T. Nguyen , C. Zhu , and Y. Liu , "A High Payload Steganographic Algorithm Based on Edge Detection", Displays Elsevier, pp. 42–51, January 2017.

[10] A. Kaur , R. Dhir and G. Sikka , "A New Image Steganography Based On First Component Alteration Technique" International journal of computer science and information security, vol. 6, 2009.

[11] H. Wu , N. Wu , C. Tsai , and M. Hwang , "An Image Steganographic Scheme Based on Pixel-Value Differencing and LSB Replacement Methods," Proceedings of the IEE Vision Images Signal Process, pp. 611–615, 2005.

[12] A. Fard, M. Akbarzadeh and F. Varasteh , "A New Genetic Algorithm Approach for Secure JPEG Steganography", Proceedings of the 2016 IEEE International Conference on Engineering of Intelligent Systems, 2006.

[13] S. Wang, B. Yang, and X. Niu , "A Secure Steganography Method based on Genetic Algorithm," Journal of Information Hiding and Multimedia Signal Processing, Vol. 1, No. 1, January 2010.

[14] H. Kanan and B. Nazeri , "A Novel Image Steganography Scheme with High Embedding Capacity and Tunable Visual Image Quality Based on a Genetic Algorithm," Elsevier Expert Systems with Applications, Vol. 41, No. 14, pp. 6123-6130, October 2014.

[15] A. Rana, N. Sharma and A. Kaur , Image Steganography Method Based on Kohonen Neural Network, vol. 2, no. 3, pp. 2234-2236, Jun 2012.

[16] N. El-Emam and M. Al-Diabat , "A novel algorithm for colour image steganography using a new intelligent technique based on three phases," Elsevier : Applied Soft Computing, August 2015.

[17] W. Chen, C. Chang and T. Le , "High payload steganography mechanism using hybrid edge detector", Expert Systems with Applications, 2010.

[18] E. Kaur, E. Mutenja, and E. Gill , "Fuzzy Logic Based Image Edge Detection Algorithm in MATLAB," International Journal of Computer Applications, Vol. 1, No. 22, pp. 57-60, 2010.

[19] H. Tseng and H. Leng , "High-payload block-based data hiding scheme using hybrid edge detector with minimal distortion," Institution of Engineering and Technology (IET) Image Processing, Vol. 8, No. 11, pp. 647–654, April 2014.

[20] T. Morkel , J. Eloff and M.S. Olivier , "An Overview of Image Steganography," Information and Computer Security Architecture (ICSA) Research Group, 2005.

[21] Z. Zhu , Tao Zhang , and Baoji Wan , "A Special Detector for the Edge Adaptive Image Steganography Based on LSB Matching Revisited", in IEEE International Conference on Control and Automation (ICCA), Hangzhou, China, pp. 1363 – 1366, 2013.

[22] W.Luo, F. Huang , and J. Huang , "Edge Adaptive Image Steganography Based on LSB Matching Revisited", IEEE Transactions On Information Forensics And Security, Vol. 5, No. 2, pp. 201-214, June 2010.

[23] Y.Lee and L.Chen , "High capacity image steganographic model", IEE Proceedings-Vision, Image and Signal Processing, Vol. 147, No. 3, pp. 288-294, 2000.

[24] N. Jain, S. Meshram, and S. Dubey , "Image Steganography Using LSB and Edge – Detection Technique," International Journal of Soft Computing and Engineering (IJSCE), vol. 2, no. 3, pp. 217 - 222, July 2012.

[25] A. Starkey, H. Hagras, S. Shakya and G. Owusu, “A Multi-Objective Genetic Type-2 Fuzzy Logic Based System for Mobile Field Workforce Area Optimization”Journal of Information Sceinces, Vol. 333, pp. 390-411, September 2016.

[26] T. Kumbasar and H. Hagras “Big Bang-Big Crunch Optimization based Interval Type-2 Fuzzy PID Cascade Controller Design Strategy “ Information Sciences, pp. 277-295, October 2014.

[27] S. Helal, J. Woong Lee, S. Hossain, E. Kim, H. Hagras and D. Cook “Persim – Simulator for Human Activities in Pervasive Spaces” Proceedings of the 2011 International Conference on Intelligent Environments, Nottingham, UK, July 2011.

[28] T. Kumbasar and H. Hagras, “A Self-Tuning zSlices based General Type-2 Fuzzy PI Controller”, IEEE Transactions on Fuzzy Systems, Vol.23, No.4, pp.991-1013, August 2015.

[29] A.Cara, C. Wagner, H. Hagras, I. Rojas and H. Pomares” Multi-objective Optimization and Comparison of Non-Singleton Type-1 and Singleton Interval Type-2 Fuzzy Logic Systems” IEEE Transactions on Fuzzy Systems, Vol. 21, No.3, pp. 459-476, June 2013.

[30] H. Hagras, M. Colley, V. Callaghan and M. Carr-West, "Online Learning and Adaptation of Autonomous Mobile Robots for Sustainable Agriculture", Journal of Autonomous Robots, Vol. 13, pp. 37-52, July 2002.

[31] H. Hagras and C. Wagner, “Introduction to Interval Type-2 Fuzzy Logic Controllers -Towards Better Uncertainty Handling in Real World Applications”, The IEEE Systems, Man and Cybernetics eNewsletter, Issue 27, June 2009.

[32] B. Yao, H. Hagras, D. Alghazzawi and M. Al haddad, “A Big Bang-Big Crunch Type-2 Fuzzy Logic System for Machine Vision-Based Event Detection and Summarization in Real-world Ambient Assisted Living” IEEE Transactions on Fuzzy Systems, 2016.

[33] A. Bilgin, H.Hagras, J. Helvert and D. Alghazzawi “A Linear General Type-2 Fuzzy Logic Based Computing With Words Approach for Realising an Ambient Intelligent Platform for Cooking Recipes Recommendation” IEEE Transactions on Fuzzy Systems, Vol. 24, No.2, pp. 306-326, 2016.