Image Steganography in Fuzzy Domain using Chromatic Adaptation Transforms (CAT)

Kirandeep Kaur[1], Kamaljit Kaur Dhillon[2]
[1]*M.Tech (CSE) Guru Nanak Dev Engineering College, Ludhiana, Punjab, India*
[2]*Assistant Professor IT, Guru Nanak Dev Engineering College, Ludhiana, Punjab, India*

Abstract - Steganography hides the very existence of a message so that if successful it generally attracts no suspicion at all. Using steganography, information can be hidden in carriers such as images, audio files, text files, videos and data transmissions. In this thesis, a new framework of an image steganography system to hide a digital text of a secret message. The main idea for this study is to use a new transform for the hiding purpose by number of bits from each pixel in an image to map them to alphabetic English characters with some special characters that are mostly using in writing a secret message. Like some steganography techniques is to hide a text of a secret message in the pixels of the image in such a manner that the human visual system is not able to distinguish between the original and the stego-image, but it can be easily performed by a specialized reader machine. Now a days, many transforms are used purposely. As this method was implemented practically on different messages and images. The carrier images that are used in the experiments of this research have no discernible change in it. Conclusion: The recorded experimental results showed that this proposed method can be used effectively in the field of steganography. Key words: Information hiding, watermarking, copyright, cryptography . The problem in the hiding information or Steganography is the size of data that user want to embed inside the multimedia file, image is one of the multimedia file, the most commend method for hiding information in the image is LSB, LSB is efficient instead of that it's not easy to analysis, however, it is not effective in term of the data hidden quantity, all researchers agreed the fact that the size of data hidden is a problem in that particular area, the other problem that faced there, in fact if we try to increase the quantity of data in the image there will be a suspect changes which become clear to human eyes, for instance, this research will face a challenge that high rate data hidden without affecting the images quality, there are many trends that needs to be fallowed, initially; how can the new algorithm increase the amount of data, then what is the feature in the new image, how can the new algorithm deal with, all this items will be discuss in-depth in this research by suggest an enhancement to the work of hiding information in the image using the human vision system.As a summery, the main problems in the Steganography fallow as: The size of data hidden, Quality of image, Algorithms that apply should also cover the gray level image., Level of data protecting and the level of suspecting.

Keywords **–** Image Steganography, Chromatic Adaptation Transforms (CAT).

I. INTRODUCTION

Steganography is the art of hiding information in ways that prevent the detection of hidden messages. Steganography, derived from Greek, literally means "covered writing." It includes a vast array of secret communications methods that conceal the message's very existence. These methods include invisible inks, microdots, character arrangement, digital signatures, covert channels, and spread spectrum communications. Steganography and cryptography are cousins in the spycraft family. Cryptography scrambles a message so it cannot be understood. Steganography hides the message so it cannot be seen. A message in ciphertext, for instance, might arouse suspicion on the part of the recipient while an "invisible" message created with steganographic methods will not. Steganography is an ancient art of hiding information. Digital technology gives us new ways to apply steganographic techniques, including one of the most intriguing that of hiding information in digital images.

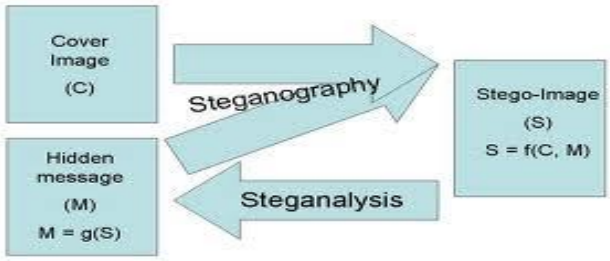

Fig.1: Steganography

II. RELATED WORKS

Steganography is the process that inserts secret messages into a cover file, so that the existence of the messages is not apparent. Research in information hiding has tremendous increased during the past decade with commercial interests driving the field (Lee, 2001). In this paper, they define zero knowledge watermark detection precisely. Then they propose efficient and probably secure zero knowledge protocols for watermarking scheme (Andre,2001). In the field of Steganography, some terminology has developed. The adjectives 'cover', 'embedded', and 'stego' were defined at the information hiding workshop held in Cambridge, England (Sellars, 2002). There are many stories about Steganography. For example ancient Greece used methods

for hiding messages such as hiding it in the belly of a hare (a kind of rabbits), using invisible ink and pigeons. Another ingenious method was to shave the head of a messenger and tattoo a message or image on the messenger head. (Davern,2002). These techniques use the message data to modulate a carrier signal, which is then combined with the cover image in section of non overlapping blocks. (S. Joshua and barett, 2002). Some Steganographic methods combine traditional Cryptography with Steganography; the sender encrypts the secret message prior to the overall communication process, as it is more difficult for an attacker to detect embedded cipher text in a cover(Sellars, 2003). This is a storage mechanism designed to give the user a very high level of protection against being compelled to disclose the file content. (Ross,2005). It aims to hide small color image inside bigger color image. It uses the transform domain in the steganography process to increase its robustness against the treatment it's done for the cover image. (N.Almayyhee, 2005). Steganography has its place in security. It is not intended to replace cryptography but supplement it. Hiding a message with Steganography methods reduces the chance of a message being detected. If the message is also encrypted then it provides another layer of protection (Johnson,2006). These tests are: Average Absolute Difference(AAD), Mean Square Error(MSE), Laplacian Mean Squared Error (LMSE),Signal to Noise Ratio(SNR), Peak Signal to Noise Ratio(PSNR), Normalized Cross-Correlation(NCC), Correlation Quality(CQ), Histogram Similarity(HS) (M. Al-Hammami,2006). It present a method to hide small Arabic texts in two cover types: the first cover is another Arabic text, where the embedding depends on the natural feature of Arabic, the second cover is an image and the process uses three methods: hiding by module 2 of LSB block, hiding by module 2 with encryption and hiding in blue channel of pixel (S. Abdullah,2006). Hidden information in the cover data is known as the "embedded" data and information hiding is a general term encompassing many sub disciplines, is a term around a wide range of problems beyond that of embedding message in content. The term hiding here can refer to either making the information undetectable or keeping the existence of the information secret. (Ingemar, 2007). The aims of this research is to study the different types of steganography systems design and implementation of steganography system which embeds information in an .exe files, the system tries to find a solution to the size of the cover file and making it detectable by anti-virus software. Software (AOS.A.Z.Ansaef, 2008). In Edge Adaptive Image Steganography Based on LSB Matching Revisited, the least-significant-bit (LSB)-based approach which is a popular type of steganographic algorithms in the spatial domain. However, we find that in most existing approaches, the choice of embedding positions within a cover image mainly depends on a pseudorandom number generator without considering the relationship between the image content itself and the size of the secret message. (Weiqi Luo,2010). A Modified High Capacity Image Steganography Technique Based on Wavelet Transform,In this study,Steganography is the art and science of concealing information in unremarkable cover media so as not to arouse an eavesdropper's suspicion. It is an application under information security field. Being classified under information security, steganography will be characterized by having set of measures that rely on strengths and counter measures (attacks) that are driven by weaknesses and vulnerabilities. (,Ali Al-Ataby1 and Fawzi Al-Naima2,2010). "Steganography Algorithm to Hide Secret Message inside an Image" In this paper, the authors propose a new algorithm to hide data inside image using steganography technique. The proposed algorithm uses binary codes and pixels inside an image. (Rosziati Ibrahim 2011). "Broadcast Steganography,"In this study of broadcast steganography (BS), an extension of steganography to the multi-recipient setting. BS enables a sender to communicate covertly with a dynamically designated set of receivers, so that the recipients recover the original content, while unauthorized users and outsiders remain unaware of the covert communication. (Fazio et.al 2013). "IMAGE STEGANOGRAPHY BASED ON CELLULAR AUTOMATA". In this paper, a new approach of image steganography using two- dimensional Cellular Automata (2D-CA) has been proposed for a confidential message. We convert the message in such a way that message length becomes 1024 bits after padding some bits. (Biswapati Jana1, Debasis Giri2, 2013).

III. CHROMATIC ADAPTATION TRANSFORMS (CATS)

Chromatic Adaptation Transforms (CATs) are used in color science and color imaging to model illumination change. Specifically, they provide a means to map *XYZ* under a reference source to *XYZ* under a target light such that the corresponding *XYZ* produce the same perceived color. The color science and imaging community has mostly adopted the linear von Kries adaptation model to compute this illumination change.

This model states that the color responses of corresponding colors under two illuminants are simple scaling apart . For example, if *RGB* and *R'G'B'* denote the color responses for an arbitrary surface viewed under two lights, then the von Kries model predicts that $R'=aR$, $G'=bG$, and $B'=cB$. In modern CATs, the scaling coefficients *a*, *b*, and *c* are the ratios of the color responses of the illuminants, i.e. $a=Rw/R'w$, $b=Gw/G'w$, and $c=Bw/B'w$. However, the CATs differ in the color space in which this scaling is applied.

IV. ALGORITHM

The proposed algorithm consists of following steps:

Step-1 : The host an secret images are acquired in jpeg format and converted to gray scale image using the following transformation:

G(r,c) = 0.2989 x R(r,c) + 0.5870 x G(r,c) + 0.1140 x B(r,c)

Where G(r,c) is the gray scale transformed image and R, G and B(r,c) are the red, green and blue color component image of the original image.

Step-2 : The gray scale transformed host and secret images are now transformed into fuzzy images using the following transformation:

$$F = \bigcup_{r=1}^{R} \bigcup_{c=1}^{C} \mu_{(r,c)}$$

Where $\mu_{(r,c)} = \frac{G_{(r,c)}}{G_{max}}$

$G_{(r,c)}$ is the gray value intensity at (r,c) location and G_{max} is the maximum gray level intensity in gray scale image.

V. RESULTS AND DISCUSSION

For Image Steganography, a jpg color image is taken as an input image. Color image gives detailed information about the fabric image and an attractive way of producing an image. JPG are the image compression standard that define procedures for compressing and decompressing images for reducing the amount of data needed to represent an image.JPG images consist of 680 * 500 pixels with bit depth 48.An image basically consists of five color objects. Clustering section are applied into image to extract pixels:-

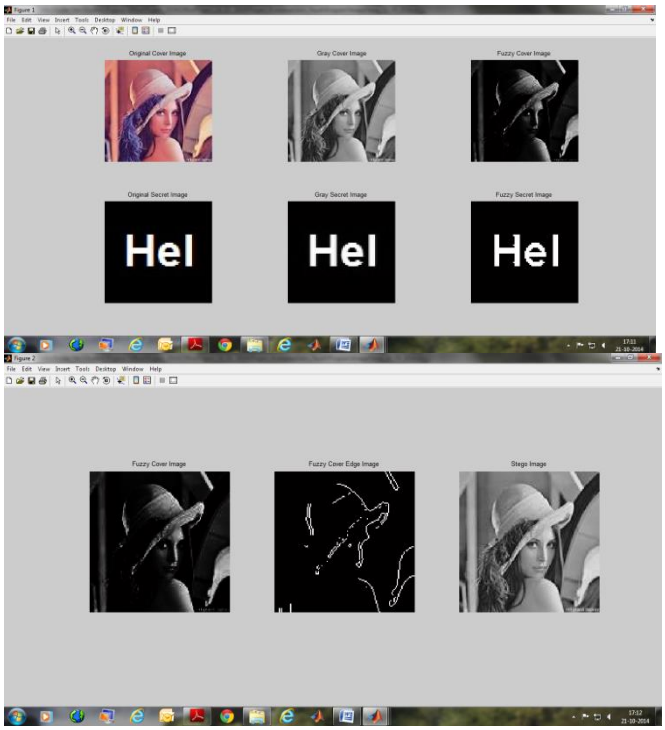

Fig.2: Results

Image Steagnography Analysis Data

Date: 21-10-2014 Time: 17-14-19

Cover Image Path = F:\1.jpg
Secret Image Path = F:\2.jpg

Imax = 255
Sigma = 45

Size of Cover Image = (126 x 126 (Row x Col)
Size of Secret Image = (64 x 64 (Row x Col)

Data Embedding Capability = 15393 bits

Size of Secret Code (Binary)= 4096 bits

PSNR = 63.454
Entropy of Cover Image = 7.607
Entropy of Cover Image = 7.606
Mean Intensity of Cover Image = 0.016
Mean Intensity of Stego Image = 0.016

After creating the cluster of a image. Cover image as shown in Figure is taken. The first is the innocent-looking image that will hold the hidden information, called the *cover image*. Fuzzy c-means (FCM) is a method of clustering which allows one piece of data to belong to two or more clusters. the original cover pixels components (H *(i, j, k))* are adjusted according to the formula as shown above .It contain the number of bits to be embedded in each coefficient. This adjustment guarantees that the reconstructed pixels from the embedded coefficients would not exceed the maximum value and hence the message will be recovered correctly.

Next image is message image. The second file is the message—the information to be hidden. A message may be plain text, cipher text, other images, or anything that can be embedded in a bit stream. Chromatic Adaptation Transforms (CATs) are used in to model illumination change as shown. Specifically, they provide a means to map *XYZ* under a reference source to *XYZ* under a target light such that the corresponding *XYZ* produce the same perceived color.

VI. CONCLUSION

In this study explored several steganography techniques and the various detection algorithms associated with them. By using the properties of the Fuzzy c means and our understanding of the chromatic adaption domain we developed new method to hide data. This new hiding method concluded easier to analyze than bit-o-steg and can hide significantly more data. Unfortunately its ease of detection makes it a less secure method. After researching various techniques already implemented, choose fuzzy method to thus creating this stego method. However, it greatly enhances the effectiveness of the steganography

since it uses a key, making it much more challenging to detect.

FCM clustering which constitute the oldest component of software computing, are really suitable for handling the issues related to understand ability of patterns, incomplete/noisy data, mixed media information, human interaction and it can provide approximate solutions faster. Currently, steganography represents a classical paradox: It is next to impossible to convince people to look for something they cannot see and do not think anyone is using because there is no large body of empirical data to prove that steganography is being used to transmit information outside of corporate networks.

VII. REFERENCES

[1] A. Bonnaccorsi, "On the Relationship between Firm Size and Export Intensity," Journal of International Business Studies, XXIII (4), pp. 605-635, 1992. (journal style)

[2] R. Caves, Multinational Enterprise and Economic Analysis, Cambridge University Press, Cambridge, 1982. (book style)

[3] M. Clerc, "The Swarm and the Queen: Towards a Deterministic and Adaptive Particle Swarm Optimization," In Proceedings of the IEEE Congress on Evolutionary Computation (CEC), pp. 1951-1957, 1999. (conference style)

[4] H.H. Crokell, "Specialization and International Competitiveness," in Managing the Multinational Subsidiary, H. Etemad and L. S, Sulude (eds.), Croom-Helm, London, 1986. (book chapter style)

[5] K. Deb, S. Agrawal, A. Pratab, T. Meyarivan, "A Fast Elitist Non-dominated Sorting Genetic Algorithms for Multiobjective Optimization: NSGA II," KanGAL report 200001, Indian Institute of Technology, Kanpur, India, 2000. (technical report style)

[6] J. Geralds, "Sega Ends Production of Dreamcast," vnunet.com, para. 2, Jan. 31, 2001. [Online]. Available: http://nl1.vnunet.com/news/1116995. [Accessed: Sept. 12, 2004]. (General Internet site)