

A Fuzzy Logic Based Techniques for content based image Retrieval and Digital Data Transmission

^[1]Dr.Ruksar Fatima, ^[2]Prof Jyoti Neginal

Abstract - Today's demand of internet in applications in large amount requires to be transmitted in a secure manner. In communication system transmission of digital data is not secure because interception and improper manipulation done by the eavesdropper. We can send digital data in such a way that no one, except the sender and the receiver can suspect the existing of data. In this paper we propose a new fuzzy logic based technique for content based image retrieval and digital data transmission, which transforms a secret digital data by embedding in another digital data with the same size and looking like selected target image. The transformation process can be controlled by a secret key generated by fuzzy logic.

Key Words— Fuzzy logic, Secret digital data, embedding, target image, carrier data.

I. INTRODUCTION

The field of image retrieval has been active research area for several decades and has been paid more and more attention in recent years as a result of dramatic and fast increase in the volume of digital images. The development of internet not only cause an explosively growing volume of digital images, but also give people more ways to get those images. The importance of an effective technique in searching and retrieving images from huge collection

cannot be overemphasized. One approach for indexing and retrieving image data is using its color and shape features [1]. Most of the CBIR systems use low level image features such as color, texture and shape for indexing and retrieval. GRAPH BASED ranking model for CBIR have been widely applied in information retrieval area [2].

Digital data from various sources are frequently utilized and transmitted through the internet from various applications, such as online personal photograph albums, confidential enterprises archives, document storage systems, medical imaging systems and military image databases. All these contain private information and they should be protected from leakages' during transmission.

Cryptography is a technique that makes use of an image, such as high redundancy and spatial correlation to get an encrypted image. The encrypted image is a noise image so that no one can obtain the secret image from it unless he/she has the correct key. Steganography is data hiding technique that hides a data in to a cover image, audio pr

video. So that no one can realize the existence of the secret data.

Thus, a main issue of the methods for hiding data, images, audio and video in other file is difficult to embed a large amount of data. If one wants to hide a secret image in to a cover image with same size the secret image must be highly compressed and data compression causes loss of data. For many application such as document storage systems, medical imaging systems and military image databases etc, that are valuable with no allowance of serious distortions.

II. RELATEDWORK

There are many papers proposed in data hiding techniques, image, audio and video steganography. Some of them summarized here.

In [3],Dr.k.sathiyasekar,S.karthick swathy Krishna proposed different data hiding techniques which includes watermarking, steganography, fingerprinting, cryptography and digital signature. In [4], Rincy MedayilJohn and Jacob Cherian proposed a secure image transmission via mosaic images using Genetic algorithm.The created mosaic image looks similar to a randomly selected target image which is used as a mask of the secret image. In [5], Usha,Srinath. N. k,Narayan and sangeeta K N proposed a secure data embedding technique in image steganography for medical images. Here confidential informations are stored in digital media and transmitted via internet. In [6], Ashalatha, anitha devi, Dr.K.B shivakumar proposed a secured secret image transmission by using fragment visible mosaic image technique to hide a secret information in a text file, image,

audio, video. In [7], Manpreet kaur, Sukhpreet kaur proposed a survey of various encryption techniques for audio data. In [8], Jithu Vimal proposed different audio steganographic techniques for hiding the information in a host audio signal. In [9], Jithya, J, Prakash, Hemand E.P proposed encryption techniques of videos. In [10], Souma Pal and prof samir kumar proposed various methods of video steganography to hide some secret information inside a video. In [11], K.ganeshkumar and. Arivazhagan proposed a cryptography algorithm with fuzzy logic for effective data communication.

III. PROPOSED SYSTEM

In the proposed system we are developing A Fuzzy Logic Based Techniques for content based image Retrieval and Digital Data Transmission to achieve the secure digital data transmission by embedding in a host file. Digital data may be a text file, image, audio or video. Host file is also a text file, image, audio or video. This will help the user to achieve the secret digital data transformation which is made invisible for the third party by exchanging the recovery codes. Our proposed system also achieves loss less data transmission and restriction less operations such as color, shape and size with less embedding time. This work also used to develop a general structure for semantic image analysis that is suitable for content based image retrieval in image search and extraction applications and architecture for its efficient implementation.

IV. MODULES

The proposed method includes three main phases:

- 1) Secret Data creation
- 2) Secret Data recovery.
- 3) CBIR

1) Secret Data creation:

In the first phase, a Secret Data is yielded, by embedding an encrypted digital data in a carrier data with additional information and a private key.

The phase includes four stages:

- a. Select digital data which we want to send and a carrier digital data where it is to be embedded.
- b. Encrypt the input secret digital data
- c. Embed the encrypted digital data with relevant information in to a carrier digital data.

2) Secret Data Recovery:

In the second phase, the embedded information and secret digital data is recovered by using private key with lossless secreta data from the generated embedded data.

The second phase includes two phases.

- a. Extract the embedded information in the carrier embedded digital data using private key.
- b. Add the information. If it matches with the embedded data then it recovers the secret digital data from the embedded carrier data.

3) CBIR:

If more than one digital data are embedded I a different carrier data paralelly, it is difficult to recognize which embedded data to send for different persons. This phase is used to recognize the embedded digital data by using CBIR.

V. POSSIBLE OUTCOMES

The proposed system transmits the secret digital data securely by embedding in a carrier data to the end user who has the proper decoding information. The carrier data consists secret information which is revealed only to the authenticated decoder without distortion and loss of data. And unauthenticated person will not get secret image instead they will get an unreadable data.

In case of user forgets in which carrier data he embedded the digital data and the sender wishes to send the particular information to a receiver, then he can apply the CBIR technique as we proposed to extract the carrier data. He will get the desired carrier data using CBIR without performing the decryption for all carrier data. Hence it will reduce the false rate effectively.

VI. REFERENCES

- [1] Reshma Chaudhari, A.M. Patil "Content Based Image Retrieval Using Color and Shape Features" Journal of Advanced reaserch in electrical, electronics and instrumentation Engineering vol.1, Issue 5, ISSN- 2278-8875, November 2012.
- [2] Bin Xu, Jiajun Bu, Chun Chen, Can Wang, Deng Cai, Xiaofei, Member IEEE, "EMR: A Scalable Graph Based Ranking Model for Content based Image Retrieval" IEEE Transaction, vol 27, No 1, Janaury 2015.

- [3] Dr.k.sathiyasekar,S.karthick swathy Krishna.K.S “ Different data hiding Techniques”, Journal of Engineering and computer science ISSN:2319-7242, vol 3, Issue 1, page no. 3655-3659 January 2014.
- [4] Rincy MedayilJohn and Jacob Cherian “A secure image transmission via mosaic images using Genetic algorithm”, IJIRST, Vol 2,Issue 5, ISSN. 2349-6010, October 2015.
- [5] Usha,Srinath. N. k,Narayan and sangeeta K N “A secure data embedding technique in image steganography for medical images”, International Journal of Advanced Research in Computer Communication Engineering, Vol 3, Issue 8, ISSN. 2278-1021, August 2014.
- [6] Ashalatha, anitha devi, Dr.K.B shivakumar “A secured secret image transmission by using fragment visible mosaic image technique”. IJANA, ISSN.0975-0282, May 2015.
- [7] Manpreet kaur,Sukhpreet kaur “A survey of various encryption techniques for audio data”. IJARCSSE, Vol 4, Issue 5, May 2014.
- [8] Jithu Vimal “Different audio steganographic techniques”. IJETT, Vol 11 ISSN. 2231-5381, May 2014.
- [9] Jithya,J,Prakash, Hemand E.P “Encryption techniques of videos” IJSETR, Vol 5, Issue 1, ISSN. 22787798, January 2016.
- [10]Souma Pal and prof samir kumar “Various methods of video steganography”. IJIRR, Vol 03, Issue 06, pp.2569-2573, June 2016.
- [11]K.ganeshkumar and. Arivazhagan “A cryptography algorithm with fuzzy logic for effective data communication”. Indian journal of science and Technology, Vol 9,ISSN.0974-5645, December 2016