Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 9, Issue, 10, pp.59153-59156, October, 2017

INTERNATIONAL JOURNAL
OF CURRENT RESEARCH

ISSN: 0975-833X

REVIEW ARTICLE

A SURVEY ON DIFFERENT FEATURES AND TECHNIQUES OF REVERSIBLE DATA HIDING

*Dilip Kumar Mishra and Yadav, S. R.

PG Head CSE, Millennium Institute of Technology, Bhopal

ARTICLE INFO

Article History:
Received 28th July, 2017
Received in revised form
11th August, 2017
Accepted 29th September, 2017
Published online 31st October, 2017

Key words:

*Digital Image Processing,
DCT, LSB, Information Extraction.*

ABSTRACT

As the digital world is growing with various kind of data like text file, image, video. Out of those image plays an important role in different field such as remote sensing, social media, etc. So the image quality is maintained by Digital image processing on various issues. This paper gives a brief survey of image data hiding techniques for various environmental scenes. Image analysis features are described in this paper with there requirements. As hiding data is data hiding but it goes under some kind of attacks which are also covered in this paper as they are the best measure for comparing different techniques of data hiding.

Citation*:* Dilip Kumar Mishra and Yadav, S. R. 2017. "A survey on different features and techniques of reversible data hiding", *International Journal of Current Research*, 9, (10), 59153-59156.

INTRODUCTION

As digital world is growing drastically people are moving towards different services provided by it. Some of these services are social network, online market. But thesetechnologies gives rise to new problem of piracy or in other words proprietary get easily stolen. In order to overcome these issues many techniques were suggested and proprietary of the digital data is preserved. So to overcome this different techniques are used for preserving the proprietary of the owner. Out of many approaches digital data embedding which is also known as digital watermarking plays an important role. Here digital information is hidden in the carrier signal which resembles the originality of the data like photographs, digital music, or digital video (Paweł Korus, 2013; Vargas, 2013; Ioan-Catalin Dragoi, 2014). One of the basic cause of the copyright issue is the easy avail ability of the internet and some software that can modify the content as per the user requirement. In few approaches inclusion of third party was done by most of the researcher where secret message is hold by one while carrier signal is hold by other (Mohan, 2013). Here embedding is done in fix part of the image where information can be hide. If fit then embedded otherwise reject. Now at extraction side image is evaluated under a calculation where it simply accept or reject image based on the obtain values. Here work has not taken measures for attacks. Watermark is broadly divided into two category first is visible watermarking and other is invisible watermarking.

In case of visible embedding watermark data is open and can be judged by naked eyes. This is shown in Fig. 1. On the other hand invisible watermarking is done in such a way that secret information is not seen or judged, so quality of the carrier signal get affected by this. This is shown in Fig. 2, although watermark data is present in the original data. Data may be of any digital information like text file, image, video file, etc. As privacy of digital data is more in case of invisible data hiding technique so popularity of this technique is quit high. As this reduce the chance of copying the watermark as well from the original signal. Although invisible embedding in carrier image is complex and challenging task but different techniques are working in this field.

Related Work

In (Ioan-Catalin Dragoi, 2014), watermark information is hidden in the edge portion of the image and for finding the exact edges pixels in the image this paper adopt DAM and BCV technique. Whole work is done for the binary image only as the DAM is based on the binary image. So here in this method image has to be in binary form and watermark information is also in binary format. With this limitation it is found that that robustness of the algorithm is quit good against different attacks of noise, filter. In (Xiaochun Cao, 2015) the extension of the paper (Ioan-Catalin Dragoi, 2014) is done where hiding is done at the edge region only using same technique of DAM and BCV but here edge selecting region is increases by searching surrounding region of the evaluating pixel. It has shown in the result that with this new approach

***Corresponding author:* Dilip Kumar Mishra**
CSE, Millennium Institute of Technology, Bhopal

robustness increases and the watermark information can be increased in the original image.

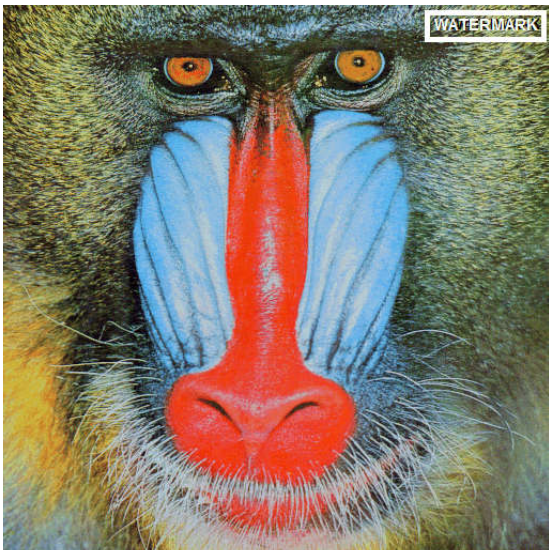

Fig. 1. Visible watermark in image data

Fig. 2. Invisible watermark in image data

In (Nallagarla.Ramamurthy, 2012), new concept is developed which is termed as content reconstruction using self embedding, here watermark image is embedded in the original image using fountain coding algorithm, where multiple packets are designed for the network. So if some of the packet get corrupted by the attack then rest of the packets are used for regenerating the original watermark. As this method cover different attacks on the image and recover watermark in original condition up to few level of attack. One problem is that after embedding image get transformed in fountain codes packet but embedded image is not available for the user to display and it get reconstructed into original only by decoding the fountain codes. So this algorithm is beneficial for data transferring purpose only. In (Elgamal, 2013) instead of embedding the external watermark image, original image is so utilize in the algorithm that it will generate its own watermark bits for the image. This paper focus on the image expansion where spatial domain is used for embedding and supporting information is stored for the image which is required during extraction. Robustness of the image is done against compression attack and scaling is also covered. But to cover both intra-codeblock and inter-codeblock methods are utilized. In [1,2] during embedding the algorithm uses DWT technique and modulus method for the pixel position selection. At the extraction end embedded image with some supporting information is supplied for generating the original image and watermark bits. This recovery of original watermark is reversible watermarking scheme. In (Priya Porwal, Apr-2014). K-SVD is adopted as the trainer. For the room preserved self embedded image generate the encrypted image i.e. by a stream cipher, such as RC4. Data Hiding in Encrypted Images: Once the encrypted image is received, the data hider can embed secret data for management or authentication requirement. The embedding process starts with locating the encrypted version of area. Since the image owner has embedded the position of the first room preserving patch and the room size for each patch in the encrypted image, it is effortless for the data hider to know where and how many bits they can modify.

Features for Data hiding

As Image is collection or sequence of pixel and each pixel is treated as single value which is a kind of cell in a matrices. In order to identify an object in that image some features need to be maintained as different object have different feature to identify them which are explained as follows:

Color feature: Image is a matrix of light intensity values, these intensity values represent different kinds of color. so to identify an object color is an important feature, one important property of this feature is low computation cost. Different Image files available in different color formats like images have different color format ranging from RGB which stand for red, green, and blue. This is a three dimensional representation of a single image in which two dimensional matrix represent single color and collection of those matrix tends to third dimension. In order to make intensity calculation for each pixel gray format is used, which is a two dimensional values range from 0 to 255. In case of binary format which is a black and white color matrix whose values are only 0 or 1. With the help of this color feature face has been detected efficiently in (Priya Porwal,Apr–2014).

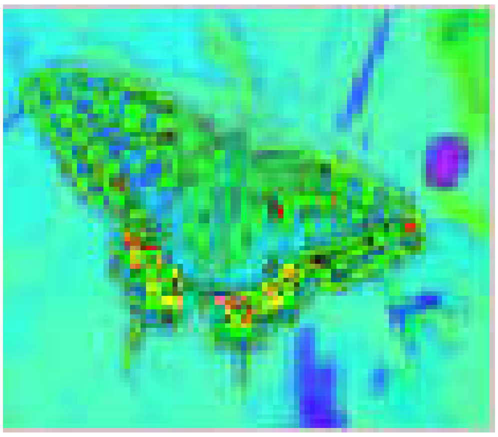

Fig. 3. Represent the HSV (Hue Saturation value) format of an image.

Edge Feature: As image is a collection of intensity values, and with the sudden change in the values of an image one important feature arises as the Edge as shown in Figure 4. This feature is used for different type of image object detection such as building on a scene, roads, etc (Nallagarla. Ramamurthy, 2012). Many algorithm has been developed to effectively point out all the images of the image or frames which are Sobel, perwitt, canny, etc. out of these algorithms canny edge detection is one of the best algorithm to find all possible boundaries of an images.

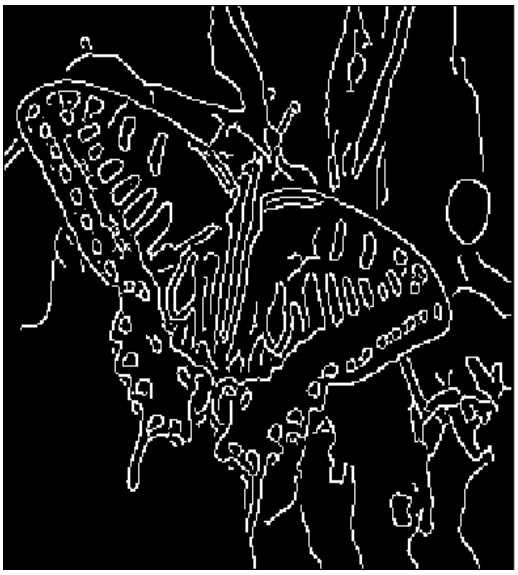

Fig. 4. Represent Edge feature of an image

Texture Feature : Texture is a degree of intensity difference of a surface which enumerates properties such as regularity and smoothness (Mr Mohan, 2013), Compared to color space model, texture requires a processing step. The texture features on the basis of color are less sensitive to illumination changes as same as to edge features.

Corner Feature: In order to stabilize the video frames in case of moving camera it require the difference between the two frames which are point out by the corner feature in the image or frame. So by finding the corner position of the two frames one can detect re-size the window in original view. This feature is also used to find the angles as well as the distance between the object of the two different frames. As they represent point in the image so it is used to track the target object.

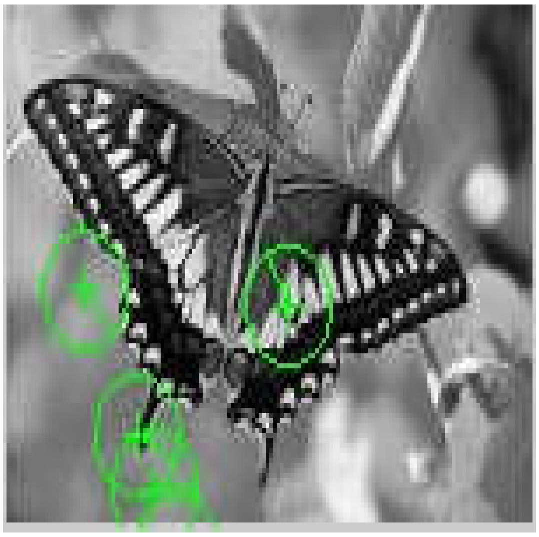

Fig. 5. Represent the corner feature of an image with green point

Watermark Attacks

As video moves from one place to another by a network. So movement of video makes various changes in the original data. So it is required that data hiding or data hiding technique should be robust against various attacks which is described in following points.

Noise Attack: This is very common problem in the transfer channel where information is sent in the data consist of some other information. So merging with other data causes small change in data which is termed as noise in the original signal. In experiment different noise producing function is used for adding these noise in the data such as : Gaussian Noise Attack, Salt & Pepper Noise, Speckle Noise Attack, etc.

Filter Attack: In this type of attack as different servers act as the mediator for passing the information from sender to receiver end so filter used in those server make few changes in the data. This is term as filter attack. In experiment same type of attack is done by applying the filters such as average filter, motion filter, sharpen filter, etc (Elgamal, 2013 and Nallagarla.Ramamurthy, 2012).

Compression Attack: In various case when data is compressed for different requirement information hidden in the video get loss. So algorithm should be protective against such type of compression attacks. Some times due to change in video format different compression algorithm uses different frame compression technique (Nallagarla.Ramamurthy, 2012). Some filtering attacks are: MP4compression, MPEG compression, etc.

Scene Swapping: This is counted as temporal attack where video frame are swapped with its own frame. In this type of attack correlation between the watermark extraction get loss and extracted frame get highly affected so data hiding algorithm which was depend on frame sequence is not robust against this attack.

Conclusions

With the high demand of image in various fields researchers get attracted for analysis. This paper cover various approaches of image data hiding. As unfavorable weather condition make high data loss, so recovering of those is done by extracting features from the image. It is also obtained that color and edge feature plays an important role for image data hiding. Here frequency based water marking technique is good for invisible embedding, but low data is embedded in the image. In future a perfect algorithm is required with good feature combination which can extract information in presence of attack as well.

REFERENCES

Angela Piper1, Reihaneh Safavi-Naini. "Scalable Fragile Data Hiding For Image Authentication". IET Inf. Secur., 2013, Vol. 7, Iss. 4, Pp. 300–311

Elgamal, A.F., N.A.Mosa, W.K.Elsaid A Fragile Video Data Hiding Algorithm For Content Authentication Based On Block Mean And Modulation Factor International Journal Of Computer Applications (0975 – 8887) Volume 80 – No.4, October 2013.

Ioan-Catalin Dragoi, Member, IEEE, And Dinu Coltuc . "Local-Prediction-Based Difference Expansion Reversible

Data Hiding". IEEE Transactions ON Image processing, VOL. 23, NO. 4, APRIL 2014.

Mr Mohan A Chimanna 1, Prof.S.R.Kho "Digital Video Data Hiding Techniques For Secure Multimedia Creation And Delivery" Vol. 3, Issue 2, March -April 2013, Pp.839-844839.

Nallagarla.Ramamurthy#1 And Dr.S.Varadarajan. "Effect Of Various Attacks On Watermarked Images. "*International Journal Of Computer Science And Information Technologies,* Vol. 3 (2), 2012,3582-3587

Paweł Korus, Student Member, IEEE, and Andrzej Dziech. "Efficient Method For Content Reconstructionwith Self-Embedding". IEEE Transactions On Image Processing, VOL. 22, NO. 3, MARCH 2013.

Priya Porwal1, Tanvi Ghag2, Nikita Poddar3, Ankita Tawde Digital Video Data Hiding Using Modified Lsb And Dct Technique. *International Journal of Research In Engineering And Technology Eissn*: 2319-1163.

Vargas L. M. and E. Vera, "An Implementation Of Reversible Data Hiding For Still Images" IEEE latin america Transactions, VOL. 11, NO. 1, FEB. 2013.

Xiaochun Cao, Ling Du, Xingxing Wei, Dan Meng, And Xiaojie Guo. "High Capacity Reversible Data Hiding In Encrypted Images By Patch-Level Sparse Representation". IEEE Transactions ON Cybernetics 2015.

****