A Survey on Various Techniques and Features of Digital Image Data hiding

Akshay Kumar Joshi[1], Sanjay Sharma[2]

[1]Research Scholar, M.Tech. in CS ,[2]H.O.D. Dept. of Computer Science, OIST, RGPV, India

***Abstract—* Data hiding is an important technique for information hiding in any digital object. Hiding technique is the science that includes communicating secret information in an appropriate digital multimedia cover objects such as audio, video and image files. Out of all those cover objects image plays an important role in different field such as remote sensing, social media, etc. So to hide the information inside the image different techniques are used. In this paper we give a brief survey on different image data hiding techniques. Image analysis features are also described in this paper with their requirements. As we know information is hidden inside the image but goes under some kind of attacks which are also cover in this paper as they are the best measure for comparing different techniques of data hiding.**

***Index Terms—* Digital Image Processing, DCT, LSB , Information Extraction.**

I. INTRODUCTION

Digital water marking is a kind of information or data hiding process by this digital data authentication is provided. This can be understand as the ease of transfer of the data from one place to another is so fast and flexible that manipulation of the original content might possible, so it might get difficult for the user or the end party that the content it using is original or not. In order to provide some procedure for checking the originality of the digital content this technique of digital data hiding has been developed. Now some important parameters which should be taken care is to balance the hiding content into the original one. This can be understand as if the original content is overload by the hiding content then chance of the original content loss is more.

Data hiding techniques has to care a lot for the complete authentication of the originality as well as without affecting the data. Whole process of authentication is done in two steps

First is embedding Algorithm here the secret information is embedded on the original content which may be image, video, etc. The secret information is any data or image, some time key is required for embedding of secret information.

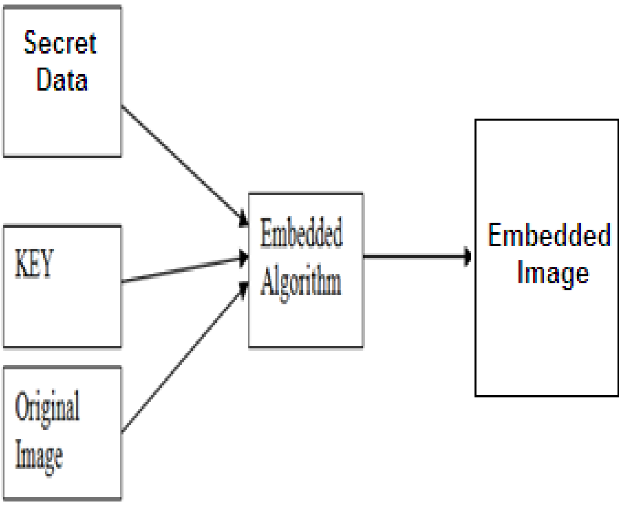

Fig.1. Embedding of Data

Other step is the Extraction of secret information from the received carrier, now if the receiver extracts secret information and that is same as the original one then received data is authentic otherwise it is unauthentic.

For a hiding algorithm to be effective, it should satisfy the following features. Imperceptibility, Robustness, hiding capacity etc.

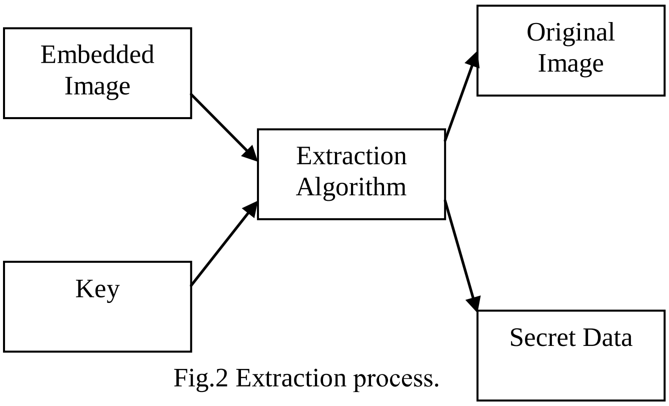

Fig.2 Extraction process.

II. REVERSIBLE AND SEPARABLE DATA HIDING

a. Reversible Data Hiding

Reversible Data Hiding is a technique that hides data in digital images for secret communication. It is a technique used for hiding additional message into cover media with a reversible manner so that the original cover content can be perfectly restored after extraction of the hidden message. Traditionally, the data hiding technique is used for secret communication of data. In some applications, the embedded carriers are further encrypted to prevent the carrier from being analyzed to reveal the presence of the embedment of data. Other applications could be for when the owner of the carrier might not want the other person, including the data hider, to know the content of the carrier before data hiding is actually performed, such as confidential medical images or military images. Here, the content owner has to encrypt the content before passing to the data hider for data hiding. The receiver can extract the embedded message and recover the original image which was used as cover image. Many reversible data hiding methods have been proposed recently.

Encryption is an effective and popular means for providing privacy. In order to securely share a secret image with other person, a content owner will encrypt the image before transmission. It may be also expected that the original content can be recovered without any error after decryption and retrieve of additional message at receiver side. Hence a reversible data hiding scheme for encrypted image is desirable.

In several cases of data hiding, the cover media will be distorted due to data hiding and cannot be inverted back to the original media. Means, cover media has permanent distortion even after the hidden data have been removed. In some applications, like medical diagnosis and law enforcement it is desired that the original cover media can be recovered efficiently with no loss. The techniques satisfying this requirement will be referred to as lossless, reversible, invertible, distortion-free or data hiding techniques [2].

b. Separable Reversible Data Hiding

As the name indicates that it is the reversible data hiding technique but which is separable. The separable means that the information hidden can be separated using suitable criteria. The activities that can be separated are extraction of original cover image and extraction of original data which was embedded. This separation exists based on the keys available. At the receiver side, three different cases are encountered viz., if encryption key is available, get the original image, if data extraction key is available, get the original data and if both the keys are available, get both data and the image. Hence it is called as Separable Reversible Data hiding.

III. RELATED WORK

In [1] new concept is develop by the paper which is term 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 packets get corrupt by the attack then rest of the packets are use for regenerating the original content. As this method cover different attacks on the image and recover content 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 reconstruct into original only by decoding the fountain codes. So this algorithm is beneficial for data transferring purpose only.

In [3] the information is hidden in the edge portion of the image and for finding the exact edge pixels in the image this paper adopt DAM and BCV technique. The DAM technique is used for identifying the optimal edge area of image for the embedding of information. The information is embedded by controlling between-class variance (BCV) which can be obtained during the process of DAM. Whole work is done for the binary image only as the DAM is work on the binary image. Here edge are used for embedding because the human visual system is insensitive to luminance change in the edge area. 1-bit of the watermark information is embedded in each edge block by changing the luminance of edge pixels, so here in this method image has to be in binary form and secret information is also in binary format.

In [10] this paper used the new concept to protect both data and image by using reversible data hiding method, encrypted data can be embedded and extracted from both encrypted images and videos. The data is encrypted using AES standard encryption algorithm and image is encrypted using by the Blowfish algorithm. After both the data and image are encrypted the embedding of data is performed by the simple LSB replacement technique. Here they use the color images for embedding , the message bits are embedded in every Red component in the RGB plane of an RGB image.

In [2] spatial common technique is use for the data hiding, here image is divide into Red, Green and Blue matrix then whole embedding is done at the blue matrix of the image where some of the LSB’s are replace by the watermark bits while rest of the MSB’s remain same. It has observed that image quality has not affected by the embedding of watermark. This paper work is robust against compression attack as it most affects the MSB’s while LSB’s remain unaffected during attack.

Detail analysis of [5]. Sparse Representation: For reserving room to hide data, we train the dictionary based on K-means singular value decomposition (K-SVD) algorithm. Dictionary Parameters Our dictionary training is based on 786 432 patches with size 4 × 4 taken from 48 standard 8-bit grayscale images in the University of Southern California, Signal and Image Processing Institute image database. For the training process, this adopt K-SVD as the trainer. In this implementation, the maximal number of iterations, T, of K-SVD is set to 50. For room reserving, work select several patches to construct a smoother area A ∈ Rn×C for room reserving, which contains C column vectors {yk}Ck =1. Here, C is the selected patch number, and the size of area A is nC. Image Encryption: For the room preserved selfembedded image Ic, we generate the encrypted image Ie 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 A. 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.

IV. FEATURES FOR DATA HIDING

As Image is collection or sequence of pixel and each pixel is treat 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 explain as follows:

Color feature: Image is a matrix of light intensity values, these intensity values represent different kind of color. So to identify an object color is an important feature, one important property of this feature is low computation cost.

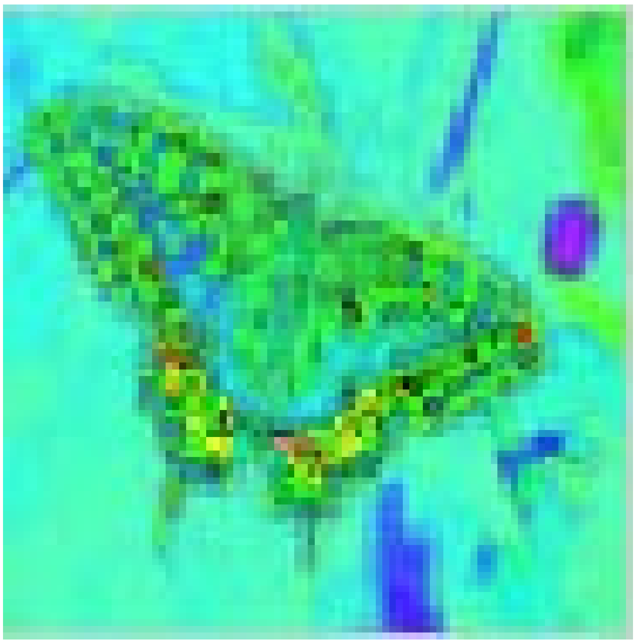

Fig. 3 Represent the HSV (Hue Saturation value) format of an image.

Different Image files available in different color formats like images have different colure 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 use, which is a two dimension 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 [8].

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 use for different type of image object detection such as building on a scene, roads, etc [7]. There are 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.

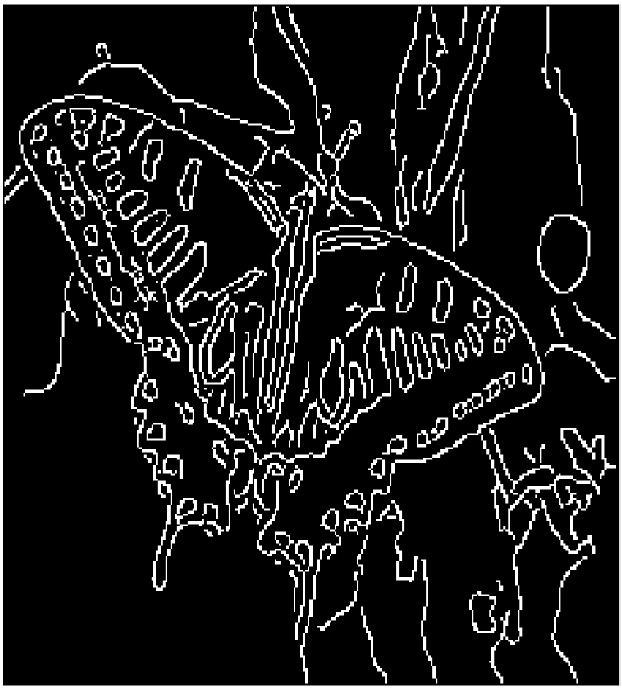

Fig. 4 Represent Edge feature of an image.

Texture Feature : Texture is a degree of intensity difference of a surface which enumerates properties such as regularity and smoothness [6]. 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 resize the window in original view. This feature is also use 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 use to track the target object.

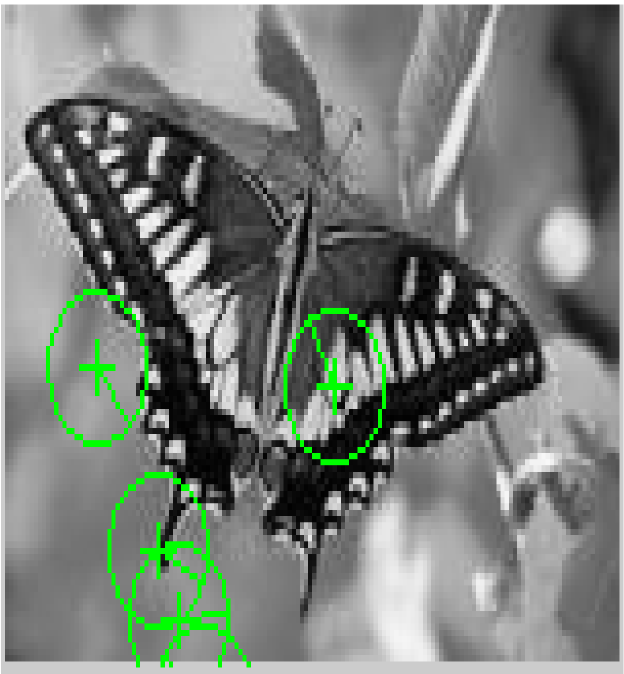

Fig 5 Represent the corner feature of an image with green point.

V. WATERMARK ATTACKS

As video move from one place to another by a network. So movement of video make 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 describe in following points.

Noise Attack: This is very common problem in the transfer of information over the channel. The content is sent which consists some other information. So during the transfer of data some noisy data is merged with original content cause small change in data which is term as noise in the original signal. In experiment different noise producing function is use 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 use 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 [6,7].

Compression Attack: In various case when data is compress for different requirement information hide in the video get loss. So algorithm should be protective against such type of compression attacks. Some time due to change in video format different compression algorithm use different frame compression technique [7]. Some filtering attacks are: MP4compression, MPEG compression, etc.

Scene Swapping: This is count as temporal attack where video frame are swap 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.

VI. 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 lose, so recovering in 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

[1] 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.

[2] L. M. Vargas And E. Vera, “An Implementation Of Reversible Data Hiding For Still Images” IEEE LATIN AMERICA TRANSACTIONS, VOL. 11, NO. 1, FEB. 2013.

[3] Kazuki Yamato, Madoka Hasegawa, Yuichi Tanaka and Shigeo Kato . “DIGITAL IMAGE WATERMARKING METHOD USING BETWEEN-CLASS VARIANCE”. 978-1-4673-2533-2/12 2012 IEEE.

[4] Angela Piper1, Reihaneh Safavi-Naini. “Scalable fragile watermarking for image Authentication”. IET Inf. Secur., 2013, Vol. 7, Iss. 4, pp. 300–311

[5] 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.

[6] A.F.Elgamal, 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.

[7] 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

[8] 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.

[9] 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.

[10] Shilpa Sreekumar, Vincy Salam Advanced Reversible Data Hiding With Encrypted Data International Journal of Engineering Trends and Technology (IJETT) – Volume 13 Number 7 – Jul 2014