© 2016 IJSRSET | Volume 2 | Issue 5 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

A Survey on various Image Water marking Techniques and Features in Digital Image Processing

Aditi Kurapa[1*], Mahendra Sahare[2]
[1]M. Tech Student of Computer Science
[2]Assistant Professor, Computer Science Department, NIIST College, Bhopal, Madhya Pradesh, India

ABSTRACT

As the digital world is growing with various kinds 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 maintain the image quality is done by Digital image processing on various issues. This paper gives a brief survey of image watermarking techniques of embedding and extraction for various environmental scenes. Image analysis features are describe in this paper with there requirements like DCT, LSB. As hiding, data is watermarking but it goes under some kind of attacks, which are also cover in this paper as they are the best measure for comparing different techniques of watermarking.

Keywords: Digital Image Processing, Embedding, Extraction, DCT, LSB.

I. INTRODUCTION

Digital water marking is a kind of information or data hiding process by this digital data authentication is provide. 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 watermarking 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.

So watermarking 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 watermark is embedded on the original content which may be image, video, etc and watermark is any data or image, sometime key is required for embedding.

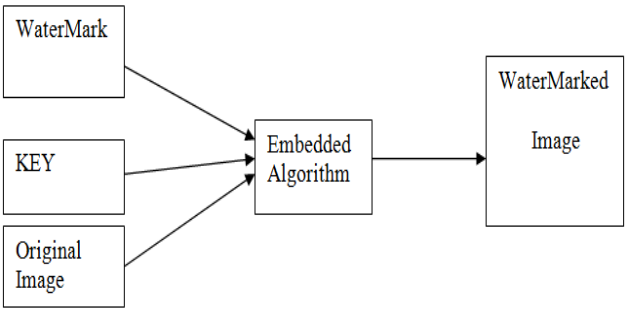

Figure 1. Embedding of watermark

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

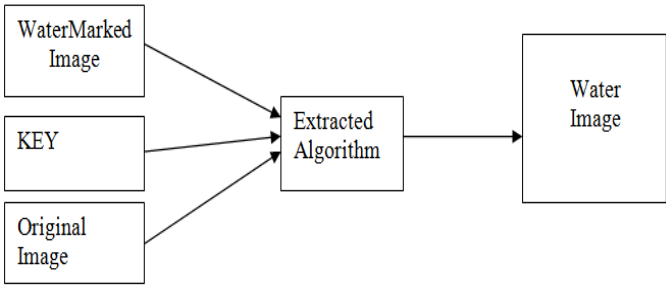

Figure 2. Extraction Process

For a watermark to be effective, it should satisfy the following features. Unobtrusive, Robustness, Subterfuge attacks, etc.

II. METHODS AND MATERIAL

A. Digital Image Watermarking Classification and Attacks

Some of the important types of watermarking based on different watermarks [3] are given below:

✓ **Visible watermarks**

This type of watermarking resembles the concept of the logos on different item to specify the product. Now these are visible in the whole data such as in case of video one constant light background or presence of logi in the video act as visible digital video watermarking, then in case of image a kind of figure appear in the image but it is not the part of the image.

✓ **Invisible Watermark**

In this type of watermarking watermark data is hide in the original data. This can be understand as some frame part which are constantly changing are those part where if small changes are made then those part is not detectable of the presence of the unrelated content so it cannot be judge by the naked eyes. This kind of watermark is known as invisible watermarking.

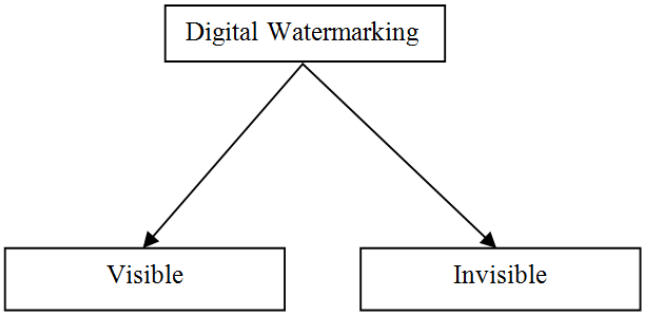

Figure 3. Different types of watermarking methodologies.

B. Related Work

Paweł Korus et. al. has introduced 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 packet get corrupt by the attack then rest of the packets are used for regenerating the original watermark [1]. As this method cover different attacks on the image and recover watermark in original condition upto 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.

Angela Piper et. al. has embedded 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 use for embedding and supporting information is store for the image, which is required during extraction [3]. Robustness of the image is done against compression attack and scaling is cover. However, to cover both intra-codeblock and inter-codeblock method is utilize.

Ioan-Catalin Dragoi et. al. has done 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 supply for generating the original image and watermark bits [4]. This recovery of original watermark is reversible watermarking scheme.

L. M. Vargas And E. Vera has spatial common technique is use for the watermarking, 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 [2].

Xiaochun Cao has done detail analysis of 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 [5]. 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.

C. Features for Watermarking

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 colure 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 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.

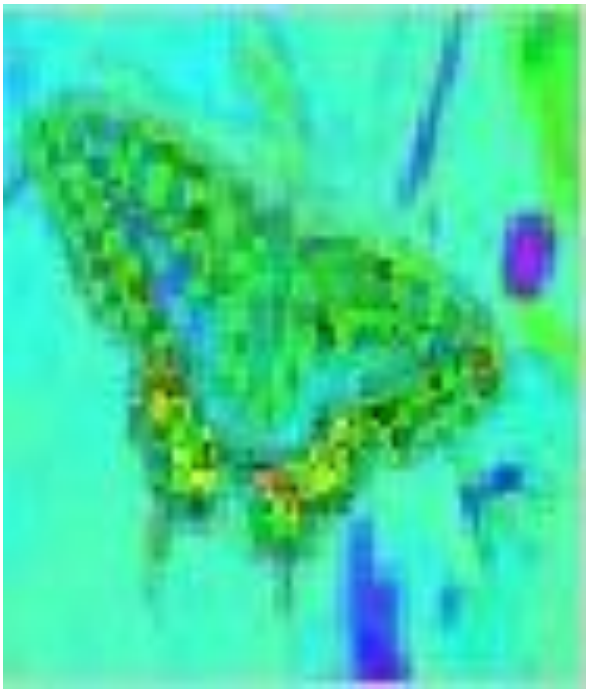

Figure 3. Represent the HSV (Hue Saturation value) format of an image.

Figure 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.

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

III. RESULTS AND DISCUSSION

A. 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 watermarking 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 channel where information is send in the data consist of some other information. So merging with other data 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 watermarking algorithm which was depend on frame sequence is not robust against this attack.

IV. CONCLUSION

With the high demand of image in various fields researchers get attracted for analysis. This paper cover various approaches of image watermarking. 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 watermarking. 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.

V. REFERENCES

[1] Pawel 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 Watermarking For Still Images" IEEE LATIN AMERICA TRANSACTIONS, VOL. 11, NO. 1, FEB. 2013.

[3] Angela Piper, Reihaneh Safavi-Naini. "Scalable Fragile Watermarking For Image Authentication". IET Inf. Secur., 2013, Vol. 7, Iss. 4, Pp. 300–311

[4] Ioan-Catalin Dragoi, Member, IEEE, And Dinu Coltuc . "Local-Prediction-Based Difference Expansion Reversible Watermarking" . IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 23, NO. 4, APRIL 2014.

[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 Watermarking 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 WATERMARKING 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 Watermarking Techniques For Secure Multimedia Creation And Delivery" Vol. 3, Issue 2, March -April 2013, Pp.839-844839.