International Journal of Computing Science and Information Technology, **2018**
ISSN: 2278-9669,April 2018 (http://ijcsit.org)

Watermarking – Review &Applications

R.Hemalatha [1].
Sindhi College,
Bangalore, India;

Priya Hari [2].
Sindhi College,
Bangalore, India,

Received January 2018

Abstract

Due to increase of internet users day by day, privacy of their data is highly required fordifferent kinds of information. One of important digital data is image, as it maintains authentication of owner. So digital watermarking came into existence, for providing security of the watermark. This paper provides a survey of different techniques of watermarking with applications. Paper has also described various attacks of watermark including geometrical and spatial category.Till date several watermarking techniques have been proposed. This paper propose a comprehensive survey of the current schemes that have been developed and their effectiveness.

Keywords: Applications, Transforms, Attacks, Color Format, Digital Watermarking

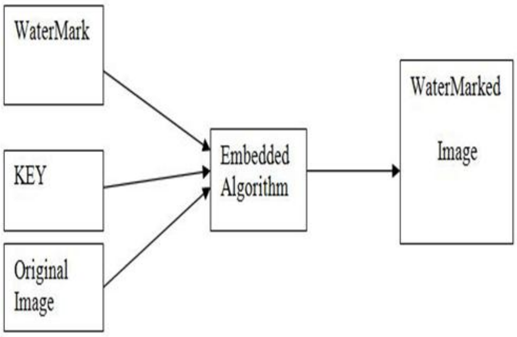
I. Introduction

As the digital world is growing drastically, people are moving towards different services provided. Few of the services are social network and online market. This technology gives rise to new problem of piracy. To overcome these, different techniques are used for preserving the proprietary of the owner. One such digital approach is watermarking which is a subsection of hiding information that is used to put some information in the original image which will specify the originality of the digital data like photographs, digital music, or digital video [1, 2, 3].In recent years, as digital media [4] are gaining wider popularity, their security related issues are becoming greater concern. Digital watermarking is a technique which allows an individual to add copyright notices or other verification messages to digital media. Image authentication is one of the applications of digital watermarking, which is used for authenticating the digital images. The objective is not to protect the contents from being copied or stolen, but is to provide a method to authenticate the image and assure the integrity of the image. The major drawback of digital signature is that it can detect if an image has been modified, but it cannot locate the regions where the image has been modified. To solve this problem, many researchers have proposed watermarking based schemes for image authentication.

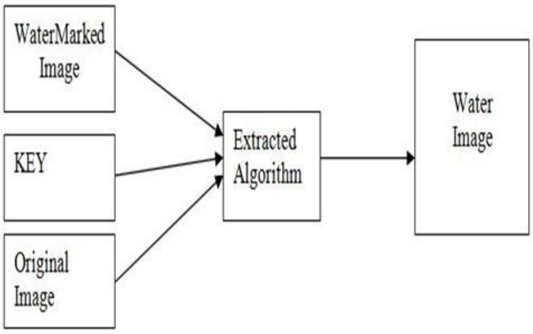
II. Watermarking Principle

A watermarking mechanism is divided into three different steps-embedding, attack and detection. In embedding process, an algorithm takes the host and the data to be embedded and obtains secreted signals. The secreted signal is then communicated, usually communicated to another person. If this person creates a modification, this is called an attack. There are several possible attacks such as noise, blurring, etc. Detection is an algorithm which is applied to the attacked signal to try to extract the watermark from it. If the signal was not modified during transmission, then the watermark is still present and it can be extracted. If the signal is imitative, then the information is also carried in the copy. The embedding takes place by working the content of the digital data, which means the info is not embedded in the frame around the data, it is carried with the signal itself. The original image and the desired watermark are embedded using one of the various schemes that are currently available. The obtained watermarked image is passed through a decoder in which usually a reverse process to that employed during the embedding stage is applied to retrieve the watermark. The different techniques differ in the way in which it embeds the watermark on to the cover object. A secret key is used during the embedding and the extraction process in order to prevent illegal access to the watermark.

Watermark is broadly divided into two categories first is visible watermarking and other is invisible watermarking. 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.



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.



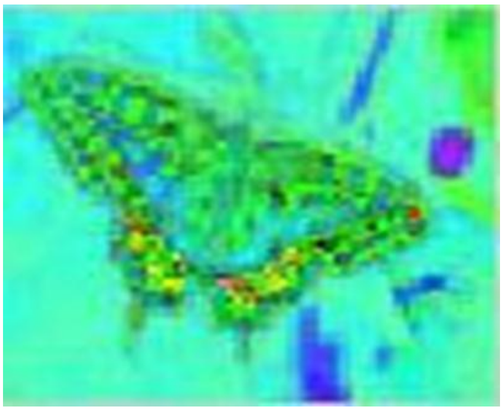
2. Extraction process.

III. Different Features

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 [5].



Represent the corner feature of an image with green point.

IV. Different Attacks

Different kind of attacks are done on the digital watermarked video, the main effect of these attack is that extraction of watermark is quite difficult or not possible by the algorithm if proper precaution is not taken in prior steps of watermark embedding.

Noise Attack: As watermarked video is send in the channel for communication then some kind of noise normally generate by which exact water is not extract from the received data [6]. Different kinds of noise are: Salt & Pepper Noise, Gaussian Noise Attack, Speckle Noise Attack, etc.

Filter Attack: Here the video will pass through different filter, which is generally done after receiving signal from the network. So this attack normally happens and for this the embedding as well as extraction algorithm of the video watermarking should be robust, so that effective method is developed. Some filtering attacks are: average filter, median filter, sharpen filter and motion filter [6, 7]. Compression Attack: Here the video will pass through different compression techniques, which is generally done after receiving signal from the network [7]. So this attack normally happens and for this the embedding as well as extraction algorithm of the video watermarking should be robust, so that effective method is developed. Some filtering attacks are: MPEG compression, Mp4 compression, etc.

Detection-disabling attacks

Sometime watermarking algorithm are based on the correlation and to make detection of the watermark so by changing this correlation make it impossible to fetch watermark from the received data. Correlation based detection and extraction fail when rotation or scaling is performed on the watermarked image because the embedded watermark and the locally generated version do not share the same spatial pattern anymore [3, 6]. Mostly, they make some geometric distortion like zooming, shift in temporal direction, rotation, cropping or pixel permutation, removal or insertion.

Ambiguity attacks

Here by introducing different watermark to confuse the detector by producing fake watermarked data to discredit the authority of the watermark by embedding several additional watermarks.

V. CONCLUSION

In this paper a comprehensive study of different watermarking techniques is explained with their requirement area. In those techniques different features of image is utilized for developing a robust algorithm. Paper has given brief explanation of the image features such as color, texture, etc. Different attacks are also explained for the awareness of the embedding and extraction algorithm. Digital watermarking research has commonly concerned on two types of watermarks, fragile and robust. Robust watermarks are made to be detected even after attempts are made to remove them. Fragile watermarks are used for verification purposes and are capable of detecting even minute variations of the watermarked content. But neither type of watermark is ideal when considering "information preserving" transformations which reserve the sense or expression of the content and "information altering" transformations which change the look of the content. To solve this difficulty a semi fragile watermark for still images that can detect information altering transformations even after the watermarked content is subjected to information preserving alterations has to be used.

REFERENCES:

[1] Haniehkhalilian, student member, IEEE, and ivan v. Bajic video ―watermarking with empirical pca-based decoding‖ ieee transactions on image processing, vol. 22, no. 12, December 2013.

[2] Paweł korus and andrzejdziech efficient method for content reconstruction with self-embedding ieee transactions on image processing, vol. 22, no. 3, march 2013

[3] X. Zhang, z. Qian, y. Ren, and g. Feng, ―watermarking with flexible self-recovery quality based on compressive sensing and compositive reconstruction,‖ IEEE trans. Inf. Forens. Security, vol. 6, no. 4, pp. 1223–1232, Dec. 2011.

[4] S. Mishra, A. Mahapatra and P. Mishra, "A Survey on Digital Watermarking Techniques", vol. 4, no. 3, (2013), pp. 451-456.

[5] M. Luby, ―lt codes in proc. 43rd symp. Found. Computer. Sci., Washington, dc, 2002, pp. 271–280.

[6] P. Korus and a. Dziech, ―a novel approach to adaptive image authentication,‖ in proc. IEEE int. Conf. Image process. Sep. 2011, pp. 2765–2768.

[7] Cheddad, j. Condell, k. Curran, and p. Mckevitt, ―a secure and improved self-embedding algorithm to combat digital document forgery,‖ signal process., vol. 89, pp. 2324–2332, Dec. 2009.