ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

A Review- Digital Watermarking

Alice Ghai[1] and Hari Om[2]

Assistant Professor, Dept. of ECE, Lovely Professional University, Jalandhar, India[1]

M.E. Student, Dept. of ECE, Punjab University, Chandigarh, India[2]

ABSTRACT: To protect or to resolve the copyright integrity, data copy, issues, multimedia, authentication techniques are used. Digital watermarking is a technique, in which some specific information, which is hard to remove, is embed with original data and transferred. It is most efficient way to protect the digital properties. Compared to the techniques and protocols for security typically employed to accomplish task, the majority of the anticipated methods based on watermarking, place a particular stress on the notion of content authentication rather than strict integrity. In this paper, analysis of various types and characteristics of watermarking techniques had carried out. Among them, we mainly focus on three processes of digital watermarking. In addition, we will examine the classification of watermarking and several applications of watermarking.

KEYWORDS: Image processing, watermarking, robust, fragile and semi fragile Watermarking

I. INTRODUCTION

Imageprocessing an image is equivalent to processing a signal for which image act as an input is an image, and the turn out of this operation is an altered image or a list of criterion put successively as a model in many situations. Processing an image determines the image in two ranges and utilizes assured image refining modes. It generally refers to digital image processing, but both analog and optical which are also image processing's are also possible [1]. The acquisition of images that is generating the input image in the first place is termed as imaging. It is an exercise of any algorithm, which takes input as an image and at the same time returns output as an image. Owed to the modern evolution in cyber automation and development of veritable immense pace, circuitry supervises all over, security of discrete appeased are essential. Therefore, security and protection of everyone's production has become a difficult task. So holding the preservation of digital watermarked expression i.e. text, audio image and video has accepted appreciable attention [2]. Watermarking is a microscopic process in which a pattern of bits is embedded with image, which is being transferred or shared. Thus, the image is completely protected and authenticated to owner. The user who knows the algorithm only can use that specified data. Digital watermarking is used for proof of ownership copying prevention authentication purpose. Watermarking technique are characterized based on persuaded properties like robustness, transparency, security, capacity, inevitability [3].

II. LITERATURE SURVEY

In a commonly coined frequency-domain watermark scheme that was propose by Cox et al. [1] in 1997, which is a spread spectrum watermark scheme. They adopt a method named spread-spectrum to introduce watermark. Then in 2000, Areealimohammed et al. [2] scheduled an adaptive watermarking method. This proposal embeds watermark in terms of a binary image in DCT approach the sable edge-analyzor method is used to access the leaning magnitude. This outcome is symmetrical to the quantity of watermarked chunk. After that in 2003, Ruisong ye et. al. [3] contemplated a Semi Fragile tide marking method in which Tellate with a PSNR OF 44DB is worn in DWT insertion domain. But in 2004, YangQianlet. al. [4] scheduled a Semi Fragile tidemarking mode in which a PSNR of 33 DB is used in DWT insertion domain. In 2006, H. Guoet. al. [5] advised a fragile tide marking topology to identify nasty improvements of knowledge bank kinship. In this proposal, all tuples in an index relation are tightly divided into groups so that modifications can be reduced in worst case. In progression, Chen et al.[6] in 2009 scheduled an approach that is dimensional estate tide marking depending on the opinion regarding standardizing chunk-wise addicted information in tide marking conduct for crimping VQ encounter without negotiating on localization potential of the scheme. In 2011, Bhattacharya et. al. [7] contemplated a unique method in which fragile and robust techniques are used to exploit the advantage of these two in combination. Then in 2011, archanaet. al. [8] conferred a amaurotic tide marking access in

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

which direction geo-dimensional statistics is protect in distinction to illicit service giving advantage of preventing from data format change data editing and random noise. In 2012, ChitlaArathiet. al. [9] conferred a semi-fragile tide marking technique that is stationed on block based SVD, that can extract the tidemark without original data. In 2012, lin et. al. [10] presented a tide marking method stationed on the density estate to elevate the deficiency of the JPEG appraisal to lessen the error rate (BER) of the extracted tidemark. In 2013, G. DayalinLeena and S. SelvaDhayanithyet. al. [11] recommended a watermarking method in which wavelet transforms is done on digital image, which is an skilled multi-resolution frequency domain approach that provides high security by using chaotic map.

III. WATERMARKING PROCESS

Three different steps, embedding, attack and detection are usually worn to perform watermarking. Watermarking system performs these steps. In embedding, the watermark signal is produce by procedure that accepts host and data to be impose. Then this signal is capture or transmitted to other user [4]. If another user performs any alteration on watermarked signal then it is coin as attack. There may be various available attacks on an image. To extract the watermark from image the algorithm is applied to the bombarded signal. This is termed as detection. During transmission, if there is no modification then the watermark is still commenced and it can be derived [5].

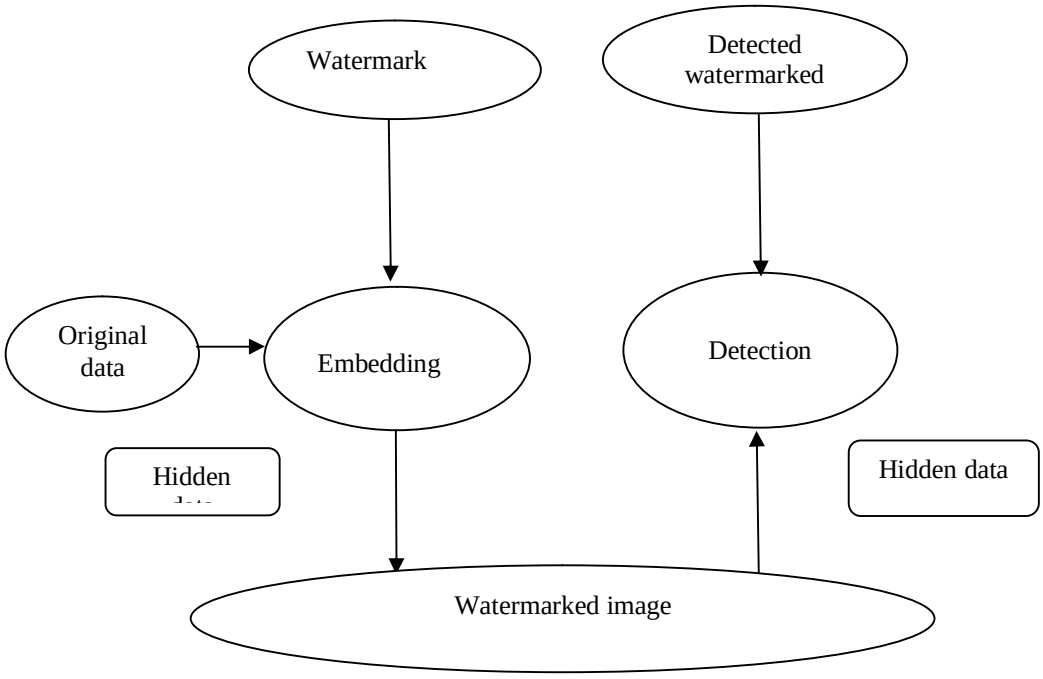

Fig 1. Block representation of Watermarking Process

Figure 3.1 represents the basic section representation of watermarking process. The original data or picture and the required tidemark are embedded using presently available. To extract the watermark decoder is used along with hidden information in reverse process opposite to embedding .

IV. CLASSIFICATION OF WATERMARKING

In these digital tidemark, appearance, their approach and pertinence are arrange and are disjoint into distinct section.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

Watermarks are also classified according to the nature which includes robust, fragile and semi fragile techniques.

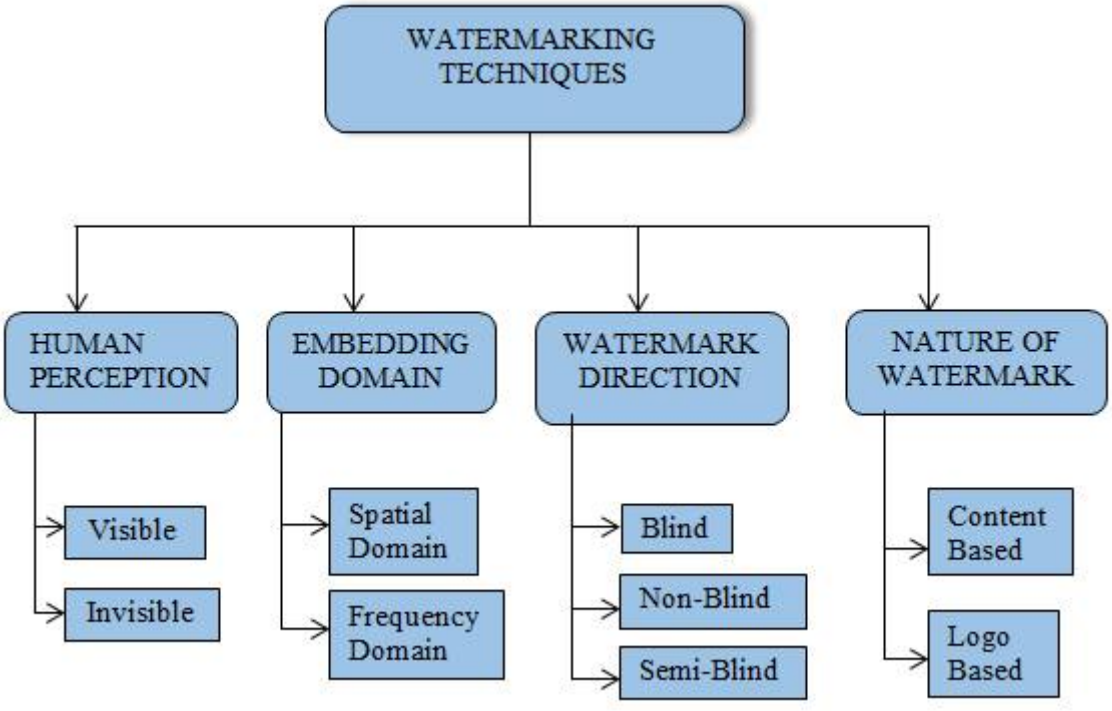

Fig 2. Classification of watermarking techniques

According to human perception:

- Visible watermark: The watermark that is detectable in the input comparable to television channels e.g. HBO, printing a watermark on paper whose logo is detect
  super imposable on the ends of the Television impression.
- Invisible watermarking: The mechanism present is accessible that may introduce information within a picture that do not detect, yet can examine including the correct software [6]. The privacy of the picture had not prohibited this course, yet it can substantiate that this is the stolen picture.

According to embedding domain:

- Spatial domain: This concentrates on customizing the picture element of one ormore uncertain preferred groups of pictures. It strictly bundles the fresh input as input to the picture element. Many of its methods are SSM LSM Intonation situated method [7].
- Frequency domain: The concern is likewise term as transmute discipline. Standard regarding assured constancies had corrected in distinction to their main. It consists of many accepted worn mutate demesne manners, such as DWT, Discrete cosine mutation as well as diverse density mutation.

According to watermark detection:

- Non blind watermarking: The concern requires a base information in the modified plan as well as secure heftiness, yet utilization is narrow [2].
- Semi blind watermarking: This needs no more a primitive data considering apprehension.
- Blind watermarking: The concern no more require primitive input, that includes deep utilization range, yet needs some greater tidemark mechanism.

According to watermark type:

- Turbulence form: This type includes Gaussian random, bogus as well as anarchic arrangement.
- Image form: This incorporates dual image, logo, imprint as well as trademark.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

According to host signal

- Image watermarking: The indicated is worn to shield the important knowledge into the image and to afterwards track down and abstract that unique knowledge for the writer‘s claim.
- Video watermarking: The mentioned casts tidemark in the video branch to sway telegenic operation. It is the expansion of image tide marking. This mechanism craves actual duration drawing and heftiness for acquiesce [8].
- Audio watermarking: This function field is one of the maximum attractive and torrid issues due to net, MP3 etc.
- Text watermarking: This casts tidemark to the DOC, PDF and extra data set to limit the adjustment formed to data. The tidemark is adding in the genesis architecture and the slots among caliber and straight zone.
- Graphic watermarking: It encloses the tidemark to either 3D or 2D processor developed visuals to demonstrate the ownership [5].

V. WATERMARKING APPLICATIONS

Watermarks embedded into digital content attend a variety of purposes. The basic applications of digital watermarking are mentioned below:

- Ownership assertion– In order to prove the copyright ownership, the owner embeds any one of his/her identification in the host media [10].
- Copyright protection– Watermarking could be used to protect reallocation of copyrighted substantial over the entrusted network such as Internet or peer-to-peer links [10]. Since the content is stamped with a visible watermark which is very hard to eliminate and it can be publicly and easily circulated.
- Content archiving– Digital contents such as images, audio or video are stored by embedding their identifications such as digital object modifier or serial number as the watermark. It gives more information about the digital content. For example an image is stored along with the information such as time and place. This information could be used for categorizingand organizing digital subjects [9].
- Broadcast monitoring– Watermarking could also be used for broadcast monitoring. In the advertisement applications, the advertising agencies can monitor whether their advertisements are essentially broadcasted at the true period and right interval.This can be achieved by embedding the watermark that is to be broadcasted together with the host media [11].
- Tamper detection – Watermarks find their advantage in tamper detection also. If the watermark is impaired or corrupted, it specifies the occurrence of tampering and hence, the digital content cannot be trusted. Tamper recognition is very significant for certain applications that include extremely delicate data like medical images [5].
- Digital fingerprinting– It is a system used to distinguish the possessor of the digital content. Fingerprints are distinctive to the vendor of the digital content. The owner inserts the fingerprint into each copy of the media [8]. Hence, a particular digital thing could have diverse fingerprints because they are appropriate to dissimilar users. The main challenge faced by fingerprinting is the collusion attack, in which numerous legal replicas of the identical media are attained.
- Copy prevention – In order to prevent illegal copying and limit the number of copies created, the owner embeds a never-copy watermark in the host media. The detector which is installed in the recording device restricts further recording.
- Authentication – The authenticity of the conventional media is verified by checking the existence of the watermark. If the watermarked media is employed, the embedded watermark becomes undetectable. Hence, the recipient would recognize that the media is inconsistent [11].
- Content integrity verification – The content is not allowed to be modified in such a way that the content meaning is altered. Embedding a watermark within the original media permits the relevant parties to confirm the integrity of the content.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

VI. CONCLUSION AND FUTURE WORK

This paper provides an absolutecritique on various digital watermarking techniques, their stipulation and relevance. The benefit of diverse type of tidemark is relevance abased. All classes of tide marking that is robust, fragile as well as semi fragile is discussed in this paper and successfully studied the different characteristics of watermarking technique.Distinctmanner for digital tide marking like overview, framework, applications, procedures, challenges along with limitations. Apart from it, a short and concerning search of watermarking procedures is scheduled with their eminence and drawback, which may be helpful in research areas.

REFERENCES

1. Cox, I. K., Kilian, J., Leighton, F. T., and Shamoon, T.,"Secure Spread Spectrum Watermarking for Multimedia," IEEE Transactions on Image Processing, Vol. 6,No. 12, pp. 1673-1687, 1997
2. A. Castillo, J. Ortegon, J. Vazquez and J. Rivera, "Virtual Laboratory for Digital Image Processing", *IEEE Latin America Transactions*, vol.12, no.6, pp. 1176-1181, 2014.
3. Ruisong Ye, "Fast Modified Signed Discrete Cosine Transform For Image Compression," Pacific-Asia Conference on Circuits, Communications and System, IEEE, pp. 485-488, May 2009.
4. Yang Qianl and CaiYanhong, "A Digital Image Watermarking Algorithm Based on Discrete Wavelet Transform and Discrete Cosine Transform," International Symposium on Information Technology in Medicine and Education, IEEE, pp. 1102-1105, August 2012.
5. H. Guo et al.," A fragile watermarking scheme for detecting malicious modifications of database relations", Information Sciences, pp.1350–1378,2012
6. Chen, D.-Y., Ouhyoung, M., and Wu, J.-L.,"A Shift-Resisting Public Watermark System for Protecting Image Processing Software," IEEE Transactions on Consumer Electronics, Vol. 46, No. 3, pp.404-414, 2000.
7. Ankan Bhattacharya, SarbaniPalit, NiveditaChatterjee, and Gourav Roy, "Blind assessment of image quality employing fragile watermarking", 7th International Sym. on Image and Signal Processing and Analysis (ISPA 2011) Dubrovnik, Croatia, pp. 431-436,2013
8. ArchanaTiwari, Manisha Sharma,"Semifragile Watermarking Schemes for Image. Authentication- A Survey", I.J. Computer Network and Information Security, pp.43-49,2012.
9. ChitlaArathi,'' A Semi Fragile Image Watermarking Technique Using Block Based SVD",International Journal of Computer Science and Information Technologies, Vol. 3 (2), 3644-3647,2012
10. T. C. Lin and C. M. Lin, "Wavelet based copyright protection scheme for digital images based on local features", Information Sciences: an International Journal, Vol. 179, Sept. 2012.
11. ChitlaArathi and DayalinLeena'' A Semi Fragile Image Watermarking Technique Using Block Based SVD",International Journal of Computer Science and Information Technologies, Vol. 3 (2), 3644-3647,2013.

BIOGRAPHY

Alice Ghai an AssistantProfessor in the Electronics and communication, Lovely Professional University. She received Master in Electronics and communication (ECE) degree in 2016 from Thapar University, Patiala, India. Her research interests are Image processing, Semi fragile watermarking etc.