International Journal of Advance Research in Science and Engineering
Vol. No.6, Issue No. 05, May 2017
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

A REVIEW STUDY ON IMAGE DIGITAL WATERMARKING AND VARIOUS TECHNIQUES

Sharanjeet Kaur [1], Vijay Kumar Banga[2]

[1]M.Tech Scholar, [2]Principal, Electronics and Communication & Engineering Department
Amritsar College of Engineering and Technology, Amritsar

ABSTRACT

Digital watermarking is the act of concealing a message associated with digital signals in several forms like a picture, song, video within the signal itself. in this paper, a review on Image Watermarking permanently strength and discuss the assorted factors utilized in watermarking, properties and application area where water making technique need to be used. additionally a survey on the some new work is completed in image watermarking field.

Keyword: — DWT, DCT, DFT, Image Transforms , Spatial Domain Watermarking.

I. INTRODUCTION

The enhanced net usage has turned a way that's able to defend the copyright of printed Medias into a necessity. The simple distribution of those documents through the online could transgress protection laws against unauthorized copies and create fidelity questionable. Digital watermarking has been proposed as an answer against these practices.

Digital watermark may be a labeling technique of digital information with secret info which will be extracted within the receptor. The image within which this information is inserted is termed cover image or host [1].

The watermarking method needs to be resilient against possible attacks, keeping the content of the watermark legible in order to be recognized once extracted. Features like strength and fidelity area unit necessities of a watermarking system, but the scale of the embedded information needs to be thought of since data becomes less strong as its size will increase. So a trade-off [2] of those options should be considered.

The paper is organized as follows. In Section II, we have a tendency to delineate the classification and every feature. In Section III, we have a tendency to justify the main applications of watermarking. A basic model and therefore the discussion concerning every block of the method that's projected in Section IV. Section V is that the conclusion and Section VI the acknowledgments.

II. BASIC OF WATERMARKING

The basic model of Digital Image Watermarking consists of two parts [9]:

1. Watermark embedding
2. Watermark extraction

International Journal of Advance Research in Science and Engineering
Vol. No.6, Issue No. 05, May 2017
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

Figure 1: Watermarking Embedding process

The first method is Watermark Embedding that's shown in Figure 1 and also the second method is that the Watermark Extraction that's shown in Figure 2.

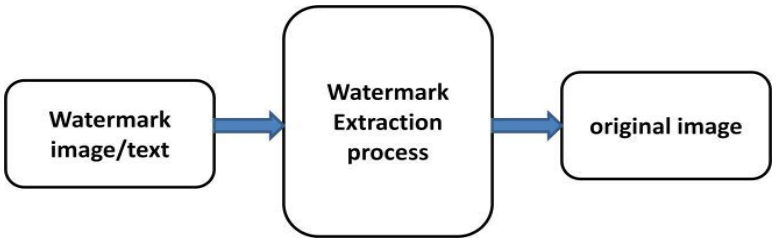

Figure 2: Watermarking Extraction Process

III. CLASSIFICATION

A watermarking system has necessities which should be met when implemented, but the application can dictate that options should be emphasized. During this section a classification of marks according with their necessities are projected.

A. Robustness:

This feature refers to the flexibility to find the watermark when some signal process operation [1]. Marks cannot survive all types of attacks, therefore attacks resilience should be optimized according to application. For example: To verify data integrity a correlation between the received image and also the signal is meted out once the watermark is extracted. If variations are found then manipulations should have occurred [3]. With that in mind the subsequent classification may be made:

1) Fragile: These marks may be destructed by tiny manipulations of the watermarked image [4]. Such marks are used for authentication and integrity verification.
2) Semi Fragile: These behave as fragile watermarks against intentional modifications and as strong watermarks against casual manipulations [5] like noise. These marks are utilized in image authentication and tamper control.
3) Robust: according to [4], these watermarks are designed to resist heterogeneous manipulations. they'll be used in copy management e observation.

B. Fidelity:

This demand may be known as invisibility. It preserves the similarity between the watermarked object and therefore the original image in line with human perception [1]. The mark should stay invisible however the incidence of tiny degradations in image brightness or contrast

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

C. Capacity or information Payload:

The number of bits that may be inserted through watermarking varies with every application. just in case of pictures, a mark are going to be a static set of bits. In videos, capability are going to be gauged by the number of inserted bits per frame, in audio files by the number of inserted bits per second [1].

D. Detection Types:

This classification determines that resources are necessary for the analysis to extract the watermark from the duvet image.

1) Blind: during this detection sort the initial image and mark data isn't accessible to the receiver. For example: Copy management applications should send completely different watermarks for every user and also the receiver should be able to acknowledge and interpret these different marks [1].

2) Non-Blind: during this case, the receiver wants the first data, or some derived information from it, for the detection method [1]. This data will be utilized in the extraction algorithmic program.

E. Embedding:

The method wont to infix the watermark influence each the strength against attacks and therefore the detection algorithmic program, however some strategies are terribly easy and can't meet the applying needs. El-Gayyar and von zur Gathen [2] showed that planning a watermark ought to take into account a trade-off among the essential options of strength, fidelity and payload.

There are 2 approaches for the embedding process:

1) **Spatial Domain:** These watermarks insert data within the cowl image ever-changing pixels or image characteristics [4]. The algorithms ought to rigorously weight the quantity of modified bits within the pixels against the possibility of the watermark changing into visible [2]. These watermarks are used for document authentication and tamper detection.

2) **Transform Domain:** These algorithms hide the water-marking data in remodel coefficients, thus spreading the info through the frequency spectrum [1] creating it hard to discover and powerful against many varieties of signal process manipulations. the foremost used remodels are: distinct cosine transform (DCT) [1], distinct wavelet remodel (DWT) [6] and distinct lifting remodel (LWT) [7].

IV. APPLICATIONS

Before discussing watermarking algorithms allow us to review some common applications:

A. Broadcast Monitoring:

This type of observance is used to verify the content that's imagined to be transmitted [1], [3], [8]. As an example, industrial advertisements may be monitored through their watermarks to verify timing and count.

B. Owner Identification:

The conventional type of intellectual ownership verification may be a visual mark. But, nowadays, this is often simply overcome by the utilization of software's that modify pictures. AN example is pictures with a copyright registration image c that have this mark removed by specialized software's. During this case invisible watermarks area unit utilized in order to overcame the matter.

C. Fingerprinting:

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

A watermarked object contains information regarding the owner permissions. many fingerprints may be hosted within the same image since the article might belong to many users [3], [8].

D. Publication observance and duplicate control:

The watermark contains owner data and specifies the corresponding quantity of copies allowed. This presupposes hardware and a software package ready to update the watermark at each use [3]. It conjointly permits copy chase of unauthorized distribution since owner data is recorded within the watermark.

E. Content Archiving:

Watermarking will be used to insert digital object symbol or serial variety to assist archive digital contents like pictures, audio or video. It may also be used for classifying and organizing digital contents. commonly digital contents are known by their file names; but, {this may be} a method as file names can be simply modified. Thus embedding the item symbol inside the item itself reduces the possibility of tampering and thus may be effectively utilized in archiving systems.

F. Meta-data Insertion:

Meta-data refers to information {|the info|the information} that describes data. pictures is labeled with its content and may be utilized in search engines. Audio files will carry the lyrics or the name of the singer. Journalists might use pictures of an event to insert the quilt story of the various news. Medical X-rays might store patient records.

G.Broadcast observation:

Broadcast Monitoring refers to the technique of cross-verifying whether the content that was imagined to be broadcasted (on TV or Radio) has very been broadcasted or not. Watermarking may be used for broadcast observation. This has major application is business publicity broadcasting wherever the entity World Health Organization is advertising needs to watch whether their publicity was really broadcasted at the correct time and for right period.

H. Tamper Detection:

Digital content may be detected for tampering by embedding fragile watermarks. If the delicate watermark is destroyed or degraded, it indicated the presence of tampering and therefore the digital content can't be trusty. Tamper detection is extremely vital for a few applications that involve sensitive data like satellite imagery | representational process or medical imagery. Tamper detection is additionally helpful in court of law wherever digital pictures might be used as a forensic tool to prove whether the image is tampered or not.

V. BASIC MODEL

Liu and He [3] present a model with 3 stages: Generation & Embedding, Distribution & possible Attacks and Detection. During this paper, we tend to adapted this model dividing the primary block in Generation and Embedding, as a result of the each use completely different watermarking algorithms and may be studied independently. The essential model planned is conferred below:

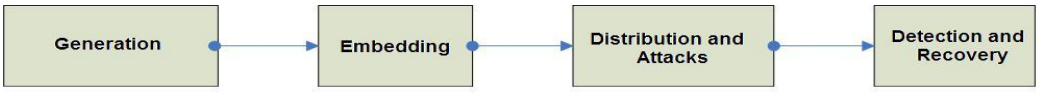

Figure 3: Basic Model

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

The explanation about the Embedding and Detection stage will be presented together, because the algorithms are related.

VI. PROPERTIES OF DIGITAL WATERMARKING

There are 3 main Properties of digital watermarking technique

A. Transparency or Fidelity: The digital watermark shouldn't have an effect on the standard of the initial image when it's watermarked. Watermarking shouldn't introduce visible distortions because if such distortions are introduced it reduces the industrial worth of the image.

B. Robustness: Watermarks might be removed on purpose or accidentally by easy image process operations like distinction or brightness sweetening, gamma correction etc. thus watermarks should be strong against kind of such attacks.

C. Capacity or Data Payload: This property describes what quantity data should be embedded as a watermark to with success observe throughout extraction. Watermark should be ready to carry enough info to represent the individuality of the image. Totally {different | completely different} application has different payload needs [10].

VII. CONCLUSION

In this paper we surveyed this literature on digital image watermarking,. we classified watermarking algorithms based on the transform domain during which the watermark is embedded. Also, study the watermarking properties, applications and techniques used. This paper shows the various techniques and discusses the necessary technology known as QR code which may be utilized in future work.

REFERENCES

[1] I. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich, and T. Kalker, "Digital Watermarking and Steganography. Morgan Kaufmann", 2008.

[2] M. El-Gayyar and J. von zur Gathen, "Watermarking techniques spatial domain" ,University of Bonn Germany, Tech. Rep., 2006.

[3] J. Liu and X. He, "A review study on digital watermarking", First Inter-national Conference on Information and Communication Technologies, pp.337–341, 2005.

[4] M. Arnold, M. Schmucker, and S. D. Wolthusen, Techniques and Applications of Digital Watermark and Content Protection. Artech House, 2003.

[5] X. Wu, J. Hu, Z. Gu, and J. Huang, "A secure semi-fragile watermarking for image authentication based on integer wavelet transform with parameters", Australasian Information Security Workshop, vol. 44, 2005.

[6] M. Antonini, M. Barlaud, P. Mathieu, and I. Daubechies, "Image coding using wavelet transform", IEEE Transaction on Image Processing, vol. 1, pp.205–220, 1992.

[7] I. Daubechies and W. Sweldens, "Factoring wavelet transforms into lifting steps", SIAM Journal on Mathematical Analysis, 1997.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

[8] V. M. Potdar, S. Han, and E. Chang, "A survey of digital image water-marking techniques", 3rd IEEE International Conference on Industrial Informatics, pp. 709–716, 2005.

[9] Ruchika Patel and Parth Bhatt, "A Review Paper on Digital Watermarking and its Techniques", International Journal of Computer Applications, vol.1, pp. 10, 13, 2015.

[10] Cox, IJ, Miller, ML & Bloom, JA 2002, "Digital Watermarking, Morgan Kaufmann Publisher", San Francisco, CA, USA 2002.