ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

IJESRT
INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A REVIEW ON VARIOUS TECHNIQUES FOR DIGITAL IMAGE WATERMARKING

Vibha Gupta*, Ekta Dixit
* Assistant Professor SSD WIT, Bathinda
Assistant Professor SSD WIT, Bathinda

DOI: 10.5281/zenodo.573516

ABSTRACT
In today's Era, message transmissions over the internet have protection problems of the digital data. Hence, protection of secret messages during transmission becomes a difficult subject. Digital watermarking is provide protection of digital information or identifying information against illegitimate exploitations and allocations. Watermarking is a technology to guarantee and make possible data certification, security and copyright defense of the information. The intend of watermarking is to consist of hidden data in multimedia information to ensure security examination. It would be then probable to progress the surrounded message, even if the information was distorted by one or more non-dangerous attacks. In this paper, we present the various types of watermarking techniques and application region where water making technique required. Also a survey on the some new work is done in image watermarking field.

KEYWORDS: Watermarking; Data Hiding; DWT; DCT; SVD; LSB.

INTRODUCTION
Protection of digital data has become a popular matter due to the quick development of the pervasive multimedia technology. Copyright protection of digital data has become a significant issue over increasing use of internet. Digital watermarking is that technology that provides security, data validation and copyright protection of the digital data. Digital watermarking is the process of embedding secret digital data, signal into the digital media such as image, video, audio and text. Later the embedded information is detected and extracted out to reveal the real identity of the digital media. Watermarking is used for Proof of Ownership, Copying Prevention, data validation, Data Hiding and Broadcast Monitoring. Digital Image Watermarking technology has many applications for protection of digital data, certification, distribution of the digital media and label of the user information. Watermarking of data has become a very important area in information hiding. This paper analyses the key technologies of Digital Image Watermarking and explore its applications and methods for the security purposes.

LITERATURE SURVEY
[1]Kilari Veera Swamy et.al., This paper presents a new compression technique and image watermarking algorithm based on Contourlet Transform (CT). For image compression, an energy based quantization is used. Scalar quantization is explored for image watermarking. Double filter bank structure is used in CT. The Laplacian Pyramid (LP) is used to capture the point discontinuities, and then followed by a Directional Filter Bank (DFB) to link point discontinuities. The coefficients of down sampled low pass version of LP decomposed image are re-ordered in a pre-determined manner and prediction algorithm is used to reduce entropy (bits/pixel). In addition, the coefficients of CT are quantized based on the energy in the particular band. The superiority of proposed algorithm to JPEG is observed in terms of reduced blocking artifacts. The results are also compared with wavelet transform (WT). Superiority of CT to WT is observed when the image contains more contours. The watermark image is embedded in the low pass image of contourlet decomposition. The watermark can be extracted with minimum error. In terms of PSNR, the visual quality of the watermarked image is exceptional. The proposed algorithm is robust to many image attacks and suitable for copyright protection applications.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

[2]M.Sreerama Murty,et.al.,The digital signature and watermarking methods are used for image authentication. Digital signature encodes the signature in a file separate from the original image. Cryptographic algorithms have suggested several advantages over the traditional encryption algorithms such as high security, speed, reasonable computational overheads and computational power. A digital watermark and signature method for image authentication using cryptography analysis is proposed. The digital signature created for the original image and apply watermark. Images are resized before transmission in the network. After digital signature and water marking an image, apply the encryption and decryption process to an image for the authentication. The encryption is used to securely transmit data in open networks for the encryption of an image using public key and decrypt that image using private key.

[3]Stephane Bounkong et.al., We present a domain-independent ICA-based approach to watermarking. This approach can be used on images, music or video to embed either a robust or fragile watermark. In the case of robust watermarking, the method shows high information rate and robustness against malicious and nonmalicious attacks, while keeping a low induced distortion. The fragile watermarking scheme, on the other hand, shows high sensitivity to tampering attempts while keeping the requirement for high information rate and low distortion. The improved performance is achieved by employing a set of statistically independent sources (the independent components) as the feature space and principled statistical decoding methods. The performance of the suggested method is compared to other state of the art approaches. The paper focuses on applying the method to digitized images although the same approach can be used for other media, such as music or video.

[4]Melinos Averkiou , Digital watermarking is the act of hiding a message related to a digital signal (i.e. an image, song, video) within the signal itself. It is a concept closely related to steganography, in that they both hide a message inside a digital signal. However, what separates them is their goal. Watermarking tries to hide a message related to the actual content of the digital signal, while in steganography the digital signal has no relation to the message, and it is merely used as a cover to hide its existence.Watermarking has been around for several centuries, in the form of watermarks found initially in plain paper and subsequently in paper bills. However, the field of digital watermarking was only developed during the last 15 years and it is now being used for many different applications.

[5]FRANK HARTUNG, et.al., Multimedia watermarking technology has evolved very quickly during the last few years. A digital watermark is information that is imperceptibly and robustly embedded in the host data such that it cannot be removed. A watermark typically contains information about the origin, status, or recipient of the host data. In this tutorial paper, the requirements and applications for watermarking are reviewed. Applications include copyright protection, data monitoring, and data tracking. The basic concepts of watermarking systems are outlined and illustrated with proposed watermarking methods for images, video, audio, text documents, and other media. Robustness and security aspects are discussed in detail. Finally, a few remarks are made about the state of the art and possible future developments in watermarking technology.

[6]Mohan Durvey et.al., This paper include the detail study of Digital watermarking explanation, concept and the main contributions in this field such as categories of watermarking process that tell which watermarking method should be used. It starts with overview, classification, features, framework, techniques, application, challenges, limitations, quality performance and performance metric of watermarking and a capable analysis of some major watermarking techniques. In the survey our most important apprehension is image only.

PROPERTIES OF WATERMARKING

The basic requirements of the digital watermarking can be treated as attributes, properties. Different applications require singular properties of watermarking. The different attributes of the watermarking take different place in application design. The basic attributes/properties of watermarking are as follows:

Robustness

Robustness refers to that the watermark embedded in data has the capability of detecting watermark after a variety of processing operations and attacks. The watermark should not removed by simple processing techniques. Hence watermark should be strong against some attack. Robust watermarks are designed to resist normal processing.

Fidelity

Fidelity or Imperceptibility is the most important requirement in watermarking system. Watermark cannot be detect by human eyes or ear, only be detected through special processing of watermark detector. It can be detected

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

by an authorized person only. Such watermarks are used for content or author validation and for detecting unauthorized copies of the data. In other words fidelity can be considered as a measure of perceptual simplicity.

Data Payload

Data payload refers to the number of bits embedded into the original image. It is the highest quantity of information that can be hidden without mortifying image quality. It can be calculated by the amount of hidden information in the original data. This property depicts how much data should be embedded as a watermark so that it can be effectively detected during extraction process.

Security

A watermark system is said to be secure, if the unauthorized person cannot remove the watermark without having full awareness of embedding algorithm, detector and composition of watermark. The security is most important factor of watermarking system. Only the authorized person can detect watermark. Thus, the copyrights protection can achieve in watermarking system.

Computational Complexity

Computation complexity is defined as the amount of time taken by the watermarking algorithm for embedding and extraction process. More computational difficulty is needed for the strong security and validity of the watermark. On the other hand, real-time applications require both speed and efficiency.

Inevitability

Inevitability defined as the possibility to produce the original data during the watermark extraction. The optimization of the parameters is mutually competitive and cannot be plainly done simultaneously. A rational negotiation is always a requirement. Alternatively, if robustness to strong warp is an issue, the message that can be frequently hidden must not be too long.

Applications of Watermarking

There are various applications of Digital Image Watermarking. These are listed as follows:

Copyright protection

The one of the most important application of watermarking is copyright protection from the unauthorized user. Ownership of digital media can be established in the case of a copyright dispute by using the embedded data as a proof.

Broadcast Monitoring

This application is used to monitor unauthorized broadcast station. It can verify whether the content is really broadcasted or not.

Tamper Detection

Fragile watermarks are used for tamper detection. If the watermark is degraded or destroyed, it indicates presence of tampering and hence digital content cannot be trusted.

Authentication and Integrity Verification

The watermark is embedded to detect if the image has customized or not, this process can be used for verification. Integrity verification can be achieved by using fragile or semi fragile watermark which has low robustness to modification in an image.

Fingerprinting

The main purpose of fingerprinting is to protect clients. If someone got a legal copy of a product, but redistributed illegally, fingerprinting can prevent this. This can be achieved by tracing the whole transaction by embedding single robust watermark for each receiver.

Content Description

This watermark can contain some detailed information of the host image such as labeling and captioning. The capacity of watermark for this kind of application should be relatively large and there is no strict requirement of robustness.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

Medical Applications

In medical field the watermarking is important for the purpose of to protect the hospital's information from unauthorized people such as patient's report etc. Security and verification of such data are now becoming very significant in medical field where the digital data are easily distributed over the internet.

Existing Techniques for Watermarking

Discrete Wavelet Transform

The basic idea of discrete wavelet transform (DWT) in image process is to multi-differentiated de-compose the image into sub images based on different spatial domain and independent frequency district. After the DWT transformation of the original image, the image is decomposed into four sub-band images with the help of DWT: three high frequency parts (HL, LH and HH, named detail sub images) and one low frequency part (LL, named approximate sub-image). HL, LH, HH are the parts with horizontal high frequency, the vertical high frequency and the diagonal high frequency part respectively and LL is the part with approximation low frequency part. The energy of the high-frequency part (horizontal, vertical and diagonal part) is less, which represent the information of the original image, such as the texture, edge, etc. The low frequency part focuses most of the power of the image to represent a significant element and it can be decomposed consistently. The power of the image is diffused better and the more powerful image strength can be included, with the more stages the image is decomposed by wavelet convert. Hence, the wavelet decomposing stages implemented in the methods can be selected as far as possible.

Discrete Cosine Transform

The Discrete Cosine Transformation is a very well-known transform function that converts a signal from spatial domain to frequency domain and it has been used in JPEG conventional for image compression due to good efficiency. As a actual transform, DCT converts actual information into actual variety and therefore prevents the issue of redundancy. The well-known block-based DCT transform sections an image non-overlapping prevent and is applicable DCT to each prevent. This outcome in providing three frequency sub-bands: low frequency sub group, mid-frequency sub-band and great regularity sub-band. DCT-based watermarking relies on two primary facts. The first one is that most of the indication power can be found at low-frequencies sub group which contains the most significant areas of the image and second one is that great frequency elements of the image are usually eliminated through pressure and disturbance strikes.

Singular Value Decomposition

The singular value decomposition (SVD) is a factorization of a actual or complicated matrix, with many useful programs in signal processing and statistics. The primary qualities of SVD from the viewpoint of image processing applications are: i) the singular values (SVs) of a image have very good balance, i.e., when a little perturbation is added to an image, its SVs do not modify significantly; and ii) SVs signify implicit algebraic image qualities.

LSB(Least Significant Bit) Technique

The LSB method the easiest method of watermark insertion. If we particularly consider still images, each pixel of the digital images has three elements — red,green and blue.

As we know that every color in the digital image is represented with one byte so it will take three bytes for representation for each pixel. Then, each color has 1 byte, or 8 pieces, in which the strength of that color can be specified on a range of 0 to 255. Now since each color is saved in another byte, the last bit in each byte shops this distinction of one. That is, the main distinction between principles 255 and 254, or 127 and 126 is saved in the last bit, known as the Least Important Bit (LSB). Since this distinction is not important much, when we substitute the color strength details in the LSB with watermarking details, the image will still look the same to the human eye. Thus, for every pixel of 3 bytes (24 bits), we can cover up 3 pieces of watermarking details, in the LSBs. To draw out watermark details, we would basically need to take all the information in the LSBs of the shade bytes and merge them.

CONCLUSION

In this survey paper we provided a recent research in the watermarking field. In this paper we have offered various characteristics for digital watermarking like basic of watermarking, techniques, applications, attacks that affects watermarking system. Copying photos from the Internet is just a matter of right clicking on a photo and saving it on the computer hence the security and authenticity of the image or data are cracks. The watermark is required to

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

prevent the original images and other documents over the internet. It is concluded that a more robust hybrid watermarking technique is required to secure the digital images.

REFERENCES

[1] Kilari Veera Swamy, B.Chandra Mohan, Y.V.Bhaskar Reddy, S.Srinivas Kumar,"Image Compression and Watermarking Scheme using Scalar Quantization", The international Journal of Next Generation Network, Vol.2, No. 1, March 2010
[2] M. Sreerama Murty, D. Veeraiah and A Srinivas Rao,"Digital Signature and Watermark Methods For Image Authentication using Cryptography Analysis",An International Journal (SIPIJ) 07/2011; 2(2). DOI: 10.5121/sipij.2011.2214
[3] Stephane Bounkong, Boremi toch, David Saad and David Lowe,"ICA forWatermarking Digital Images", Journal of Machine Learning Research 4 (2003) 1471-1498
[4] Melinos Averkiou, Digital Watermarking,2010
[5] Frank Hartung, Jonathan K. Su, and Bernd Girod,"Spread Spectrum Watermarking: Malicious Attacks and Counterattacks", Jan 1999
[6] Mohan Durvey, Devshri Satyarthi,"A Review Paper on Digital Watermarking", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 3, Issue 4, July-August 2014
[7] Haowen Yan, Jonathan Li, Hong Wen ,"A key pointsbases blind watermarking approach for vector geospatial data", Proceedings of Elsevier Journal of Computers, Environment and Urban Systems, 2012, Volume 35, Issue 6, pp. 485–492.
[8] Huang-Chi Chen, Yu-Wen Chang, Rey-Chue Hwang "A Watermarking Technique based on the Frequency Domain", Proceedings of Journal of Multimedia, 2012,Vol. 7, No. 1, pp. 82-89.
[9] A. Kannammal, K. Pavithra, S. Subha Rani, "Double Watermarking of Dicom Medical Images using Wavelet DecompositionTechnique", Proceedings of European Journal of Scientific Research, 2012, Vol. 70, No. 1, pp. 46-55.
[10] Manpreet kaur, Sonia Jindal, Sunny behal, " A Study of Digital image watermarking" , Proceedings of Volume2, Issue 2, Feb 2012.
[11] G. Dayalin Leena and S. Selva Dhayanithy, "Robust Image Watermarking in Frequency Domain", Proceedings of International Journal of Innovation and Applied Studies ISSN 2028-9324 Vol. 2 No. 4 Apr. 2013, pp. 582-587
[12] Ankan Bhattacharya, Sarbani Palit, Nivedita Chatterjee, and Gourav Roy "Blind assessment of image quality employing fragile watermarking", Proceedings of 7th International Sym. on Image and Signal Processing and Analysis Dubrovnik, Croatia, 2011, pp. 431- 436.G

CITE AN ARTICLE

Gupta, V., & Dixit, E. (2017). A REVIEW ON VARIOUS TECHNIQUES FOR DIGITAL IMAGE WATERMARKING. *INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY, 6*(5), 476-480. doi:10.5281/zenodo.573516