IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 11, Issue 6, June 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 || A Monthly Peer Reviewed & Referred Journal |

|| Volume 11, Issue 6, June 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1106076 |

Watermarking Techniques for Secure Data Transfer (A Review)

Prof. Saurabh Verma[1], Prof. Abhishek Vishwakarma[2], Ayush Tiwari[3], Om Kesharwani[4]

Department of Computer Science & Engineering, Baderia Global Institute of Engineering & Management, Jabalpur, Madhya Pradesh, India[1,2,3,4]

ABSTRACT: One of most important property of digital information is that it is in principle really easy to produce and distribute unrestricted number of its copies. The actuality that an unlimited number of ideal copies of text, audio and video data can be illegally distributed and produced requires to study ways embedding copyright information and serial number in audio and video data Now a day's internet is an necessary channel for digital assets, but it has been noticed that everybody are misusing by building illegal copies and leaking the information which creates a bad atmosphere in the field of software industry .It can be avoided by doing most outstanding efforts using digital watermarking. As we have witnessed in the past many months, the problem of protecting multimedia information becomes more essential and a lot of copyright owners are worried about protecting any illegal duplication of their data or work. Some serious work wants to be performing in order to maintain the accessibility of multimedia information but, in the meantime the industry must come up with ways to guard brain property of makers, distributors or simple owners of such data. [1] Of the many approaches possible to protect visual data, digital watermarking is probably the one that has received nearly all interest. We know that stenography and watermarking are main specifics of quick developing area in case of information hiding. Generally Watermarks are used where authentication or ownership is compulsory. Watermarks are a good way by which anyone can verify the ownership of multimedia. This paper attempts to first introduce digital watermarking as well as some of its essential notions. It is followed by describing some applications of watermarking techniques.

KEYWORDS: DWT, DCT, SVD, PSNR, MSE, NC

I. INTRODUCTION

Today's generation is eyewitness of developments of digital media. A very simplest instance of digital media is a photo captured by phone camera. The use of Digital media is frequent in present era. Other example of Digital media is text, audio, video etc. We identify an internet is the fastest medium of transferring data to any part in a world. As this technology grown-up the threat of piracy and copyright very clear thought is in owners mind. So Watermarking is a process of protected data from these threats, in which owner identification (watermark) is merged with the digital media at the sender end and at the receiver end this owner ID is used to recognize the authentication of data. This technique can be useful to all digital media types such as image, audio, video and documents. From past many years researchers and developers worked in this area to increase best results[1].

II. NEED OF WATERMARKING

Watermarking methods are based on the human image system in which it cannot be accepted due to tiny differences. In these Techniques, the cover-image is used to hide the secret information and the stego - image is the cover image with the secret data embedded inside. It hides the undisclosed information in general files secretly first and then transmits these files through network, because they look the same as broad files, they can escape from the attention of illegal interceptors easily and therefore the secret information is not easy to be attacked.

III. PRINCIPLE OF WATERMARKING

A watermarking system is frequently divided into three distinct steps, embedding, attack and detection. In embedding, an algorithm accepts the host and the data to be embedded and produces a watermarked signal. The watermarked signal is then transmitted or stored, generally transmitted to another person. If this person makes a modification, this is called an attack. There are many probable attacks. Detection is an algorithm which is applied to the attacked signal to attempt to extract the watermark from it. If the signal was not modified during transmission, then the watermark is still nearby

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 || A Monthly Peer Reviewed & Referred Journal |

|| Volume 11, Issue 6, June 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1106076 |

and it can be extracted. If the signal is copied, then the information is also carried in the copy. The embedding takes place by manipulating the substance of the digital data, which means the information is not embedded in the frame in the region of the data, it is carried with the signal itself[2].

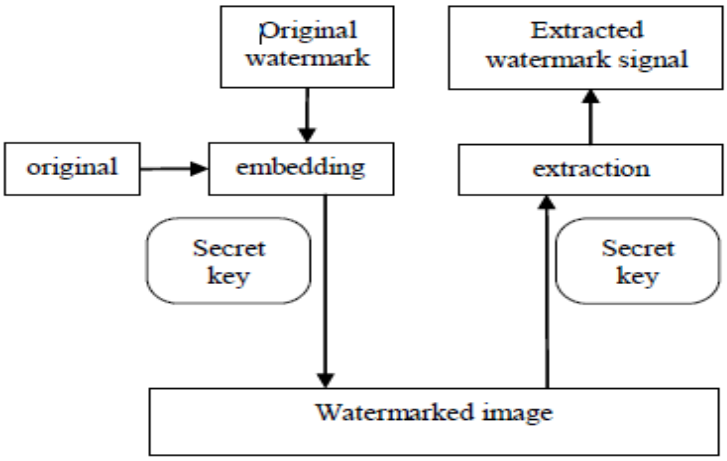

Fig. 1 Block diagram of Watermarking Process

IV. APPLICATIONS

Applications of watermarking are following:

4.1 Broadcast monitoring

In 1997, a scandal broke out in Japan regarding television advertising. At least two stations had been usually overbooking air time. Advertisers were paying for thousands of commercials that were in no way aired [17]. The practice had remained largely undetected for over twenty years, in part because there were no systems in position to monitor the actual broadcast of advertisements. There are numerous types of organizations and individuals interested in broadcast monitoring. Advertisers, of route, want to ensure that they receive the air time purchased from broadcasting firms. Musicians and actors want to make sure that they receive exact royalty payments for broadcasts of their performances.1 And copyright owners want to make sure that their property is not illegally rebroadcast by pirate stations. We can use watermarks for broadcast monitoring by putting a irreplaceable watermark in each video or sound clip prior to broadcast. Automated monitoring stations can then receive broadcasts and look for these watermarks, identifying when and where each clip appears. Viable systems have been deployed for a number of years and the basic concepts have a long history [16, 3, 20, 12, 4].

4.2 Owner identification

Although a copyright notice is no longer essential to guarantee copy rights, it is still suggested. The form of the copyright notice is usually “date, owner”. On books and photographs, the copyright is located in plain sight. In movies, it is appended to the end of the credits. And on prerecorded music, it is placed on the packaging. One drawback of such text copyright notices is that they can often be removed from the protected material. A recent spot-check by the Screen Actor’s Guild found an average of $1000 in underpaid royalties per hour of United State television programming [2]. The earliest orientation we have found [16] is assigned to the Muzak Corporation, famous for providing “elevator music”, and may be the source of the many rumors that Muzak contained subliminal messages. 1 Packaging can be lost, movies can have the credits cut off, and images can be spatially cropped. A digital watermark can be used to provide complementary copyright marking functionality because it becomes an important part of the content, i.e. the copyright information is embedded in the music to addition the text notice printed on the packaging. The Digimarc corporation has marketed a watermarking system designed for this application. Their watermark embedder and detector are bundled with Adobe’s popular image processing program, Photoshop. When the detector finds a watermark, it contacts a central database to identify the watermark’s owner (who must pay a fee to keep the information in the database).

4.3 Proof of ownership

Multimedia owners may would like to use watermarks not just to identify copyright ownership, but to actually prove ownership. To illustrate the problem, let’s speedily introduce some characters who are well known in the watermarking literature. Suppose Alice creates an image and puts it on her website, with a copyright notice “c Alice 2000”. Bob then

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 || A Monthly Peer Reviewed & Referred Journal |

|| Volume 11, Issue 6, June 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1106076 |

steals the image, uses an image processing program to switch the copyright notice with "cBob 2000", and then claims to own the copyright himself. How can the argument resolved? Traditionally, Alice could register the image with the Copyright Office by sending a copy to them. The Copyright Office archives the image, jointly with information about the rightful owner. When the dispute between Alice and Bob comes up, Alice contacts the Copyright Office to obtain proof that she is the fair owner. If Alice did not register the image, then she should at least be able to show the film negative. However, with the rapid recognition of digital photography, there might never have been a negative. In theory, it is possible for Alice to use a watermark embedded in the image to verify that she owns it. However, this is not a trivial problem, as Craver et al [11] have noted.

4.4 Authentication

As both still and video cameras progressively more embrace digital technology, the ability for imperceptible tampering also increases. The content of digital photographs can easily be altered in such a way that it is very difficult to detect what has been changed. In this case there is not even an unique negative to examine. There are many applications where the veracity of an image is crucial, especially in legal cases and medical imaging. Validation is a well studied problem in cryptography [23]. Friedman [13, 14] first discussed its application to create a "trustworthy camera" by computing a cryptographic signature that is linked with an image. If even one bit of one pixel of the image is modified, it will no longer match the signature, so any tampering can be detected. However, this signature is metadata that must be transmitted along with the photograph, perhaps in a header field of a specific image format. If the image is subsequently copied to another file format that does not contain this header field, the signature will be lost, and the image can no longer be valid. A preferable solution is to embed the signature directly into the image using watermarking. This eliminates the problem of ensuring that the signature stays with the image. It also opens up the possibility that we can learn more about what tampering has occurred, since any changes made to the image will also be made to the watermark. Thus, there are several systems that can indicate the rough location of changes that have been made to the image. There are also systems designed to allow certain changes, such as JPEG compression [18, 19], and only disallow more substantial changes, such as removing an individual from a crime scene.

V. CLASSIFICATION OF DIGITAL WATERMARKING

Here we will discuss different categories of watermark, characteristics, techniques and their applications. According to robustness

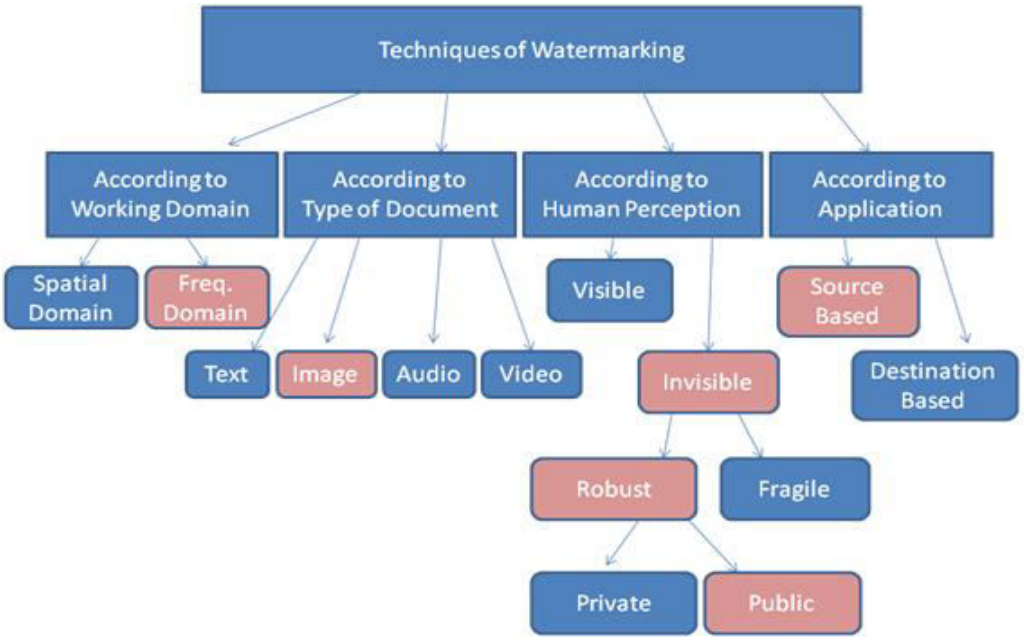

Fig 2: Types of Watermarking

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 || A Monthly Peer Reviewed & Referred Journal |

|| Volume 11, Issue 6, June 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1106076 |

5.1 Fragile watermarking:
It is used for integrity protection, which must be very sensitive to change of signal. According to state of fragile watermark, one can predict whether the original data has been tampered or not.

5.2 Semi Fragile watermarking:
It is capable of tolerating some degree of change to watermarked image like addition of noise attacks [6].

5.3 Robust watermarking:
It is mainly used to prevent various noisy attacks, geometrical or non-geometrical attacks without tampering embedded watermark. So the watermark is not destroyed after some attacks and can easily detected to provide certification.

5.4 According to perceptivity

5.4.1. Visible watermarking:
It is visible in digital data e.g. HBO, where logo is visibly superimposed on the corner of TV picture [5].

5.4.2. Invisible watermarking:
By this technology, we can insert the secret information into digital media like image which cannot be seen. It must be extracted by specific process.

5.5 According to attached digital signal

5.5.1. Image watermarking:
It is used to embed particular original data into digital image

5.5.2. Video watermarking:
It embeds the original data in the video stream. It requires real time extraction [2]

5.5.3. Audio watermarking:
Here we use the audio system for watermark like MP3. 2.4 According to task performed Data authentication and integrity

5.5.4. Image Watermarking:
It keeps the contents of image same as it was at initial stage. It prevents the lossy compression Copyright protection

5.6 According to domain type

5.6.1. Spatial watermarking:
This domain emphasis on modifying the one or two randomly choosed subsets of image for directly loading the raw data into the pixels. Some of algorithms used in this domain are LSB, SSM modulation based techniques. Computational complexity in spatial domain is low and it is mainly used in authentication.

5.6.2. Transform watermarking:
It is also called frequency domain. In this domain value of certain frequencies are changed from their initial values.DCT, DWT, DFT are few commonly used frequency domain method. Computational complexity in this method is high. It is used in copyright application

5.7 According to extraction process
5.7.1. Visual watermarking: It has stronger robustness but its application is limited
5.7.2. Semi-blind watermarking: There is no need of original media for detection and extraction.
5.7.3. Blind watermarking: It requires a higher watermark technology and does not need original data.

5.8 According to secret keys
5.8.1. Asymmetric watermarking: For embedding and detecting the watermark, different keys are used.
5.8.2. Symmetric watermarking: Here we use the same keys for both embedding and detecting the watermark

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 || A Monthly Peer Reviewed & Referred Journal |

|| Volume 11, Issue 6, June 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1106076 |

VI. TECHNIQUES USED IN WATERMARKING FOR DIGITAL IMAGES

From the literature and survey of various watermarking techniques There are basically two watermarking schemes namely, spatial domain and frequency domain. In spatial domain, the watermark is embedded by changing the pixel values of the original image. In frequency domain, the watermarks embedded by changing the values of its transform coefficients.

Spatial Domain Techniques: Watermark in spatial domain technique is inserted in the cover image and changing pixels value. Against the possibility of the watermark becoming visible the algorithm should carefully weight the number of altered bits in the pixels value [12].Frequency Domain Techniques: Frequency-domain methods are more idely applied as compared to spatial - domain methods. The aim of watermarks in the spectral coefficients of the image is embedded. In frequency domain Mostly used transforms are the

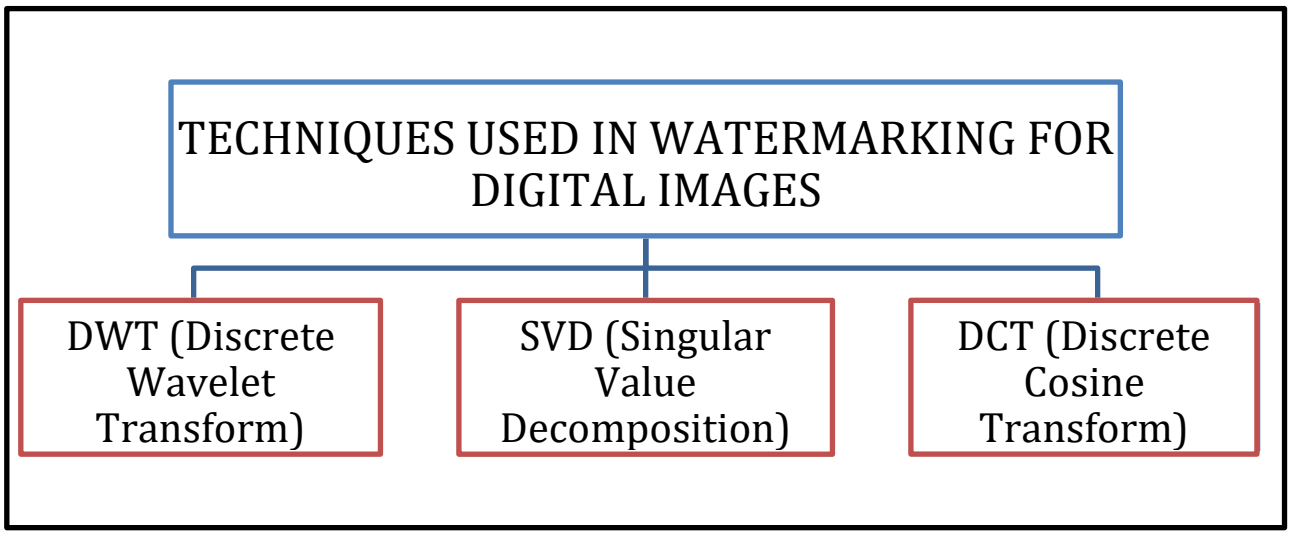

Fig 3: TECHNIQUES USED IN WATERMARKING FOR DIGITAL IMAGES

6.1 Discrete wavelet transform: Discrete wavelet transform (DWT) is a neoteric technique consecutive used in digital image processing, compression, digital watermarking etc [14]. Discrete wavelet transform is more efficient than discrete cosine transform method. The image is dissolved into high and low frequency elements in two level discrete wavelet transform (DWT). The robustness with respect to divers attacks increases when the watermark is embedding in low frequencies gained by WD (wavelet decomposition). Now first digital media is segmented into frames, Then discrete wavelet transform is applied to luminance element of each frame which outcomes into discrete sub bands. Again these bands are dissolved into discrete components. Now covariance matrix is calculated for each component. Now watermarked luminance component of the frames are gained by applying inverse discrete wavelet transform. Ultimately watermarked digital media is gained by renewing the watermarked frame [14, 3].

6.2 Singular value decomposition: Singular value decomposition is a rousing numerical technique which is utilized to diagonally matrices in numerical analysis [15]. In variety of applications singular value decomposition is used as an algorithm. In this singular value decomposition transformation, One matrix can be dissolved into three matrices. These matrices are of the equal size as the original matrix. By the linear algebra, an image is an array of nonnegative entries of scalar values that can be deduced as a matrix. Sine tort of important component, Assume if formula is where A is a square image, R is the real number domain, Then singular value decomposition of A is denoted as . Here U and V both are orthogonal matrices, and diagonal matrix is S, as

Here diagonal components i.e. s's are singular values and satisfy S1≥S2≥…....Sr≥Sr+1≥??……..??Sn??0 Singular value decomposition is an optimal matrix decomposition technique in a least square sense that it grids the highest signal energy into some coefficients as feasible [16].

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 || A Monthly Peer Reviewed & Referred Journal |

|| Volume 11, Issue 6, June 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1106076 |

VII. CONCLUSION

Digital watermarking is a technology that manages and assigns data authentication, security, and copyright security to the digital information. Digital watermarking algorithms are divided into two groups. One technique is spatial domain. In this techniques pixel values straightly works. The Second is frequency domain techniques employ several transforms, either local or global. Various widely recognized techniques are described consequently [12].

REFERENCES

[1] H.-T. Wu and Y.-M.Cheung,"Reversible watermarking by modulation and securityenhancement," IEEE Trans. Instrum. Meas., vol. 59, no. 1, pp. 221–228, Jan. 2010.
[2] F. Hartung and M. Kutter, "Multimedia watermarking Technique", IEEE proceeding on Signal Processing", Volume 87, NO.7, pp.1079-1107, July 1999.
[3] C. I. Podilchuk and E. J. Delp, "Digital Watermarking:Algorithms and Applications," IEEE Signal Processing Magazine, , pp. 33-46, July 2001.
[4] R. G.vanSchyndel, A. Z. lTrkel and C.F.Osbome, "A Digital Watermark" IEEE, 1994.
[5] J. Sang and M. S. Alam,"Fragility and robustness of binary-phase only filter- basedfragile/semi-fragile digital image watermarking," IEEE Trans.Instrum. Meas., vol. 57, no. 3,pp. 595–606, Mar. 2008.
[6] L.B. Almeida, "An introduction to the angular Fourier transform," Acoustics, Speech, and Signal Processing, 1993. ICASSP-93, 1993 IEEE International Conference on , vol.3, pp.257-260, Apr 1993.
[7] L.B. Almeida, "The fractional Fourier transform and time-frequency representations ," Signal Processing, IEEE Transactions on , vol.42, no.11, pp.3084-3091, Nov 1994.
[8] A.I. Zayed, "On the relationship between the Fourier and fractional Fourier transforms," Signal Processing Letters, IEEE , vol.3, no.12, pp.310-311, Dec 1996.
[9] Chen Wen-Hsiung, C.Smith, S.Fralick, "A Fast Computational Algorithm for the Discrete Cosine Transform," Communications, IEEE Transactions on , vol.25, no.9, pp. 1004- 1009, Sep 1977.
[10] Jianmin Jiang and GuocanFeng , "The spatial relationship of DCT coefficients between a block and its sub-blocks," Signal Processing, IEEE Transactions on , vol.50, no.5, pp.1160-1169, May 2002.
[11] H. Lim, C. Yim, E.E. Swartzlander Jr., "Finite Word-Length Effects Of An Unified Systolic Array For 2-D DCT/IDCT", 1996 IEEE International Conference on Application-Specific Systems, Architectures and Processors (ASAP'96).
[12] A. Nikolaidis and I. Pitas, "Asymptotically optimal detection for additive watermarking in the DCT and DWT domains," IEEE Trans. Image Process., vol. 12, no. 5, pp. 563–571, May 2003.
[13] S. Mallat, "The theory for multiresolution signal decomposition: The wavelet representation," IEEE Trans. Pattern Anal. Mach. Intell., vol. 11, no. 7, pp. 654–693, Jul. 1989.
[14] Andrew B. Watson, Gloria Y. Yang, Joshua A. Solomon, and John Villasenor,"Visibility of Wavelet Quantization Noise", IEEE Transactions on image processing ,Vol. 6,No. 8, August 1997.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.379

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details