INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 6.078
(Volume 6, Issue 3)
Available online at: www.ijariit.com

Security issue in watermarking: An overview

Mansi
mansisinghal63@gmail.com
Bhagat Phool Singh Mahila Vishwavidyalaya, Sonipat, Haryana

ABSTRACT

This paper provides the conceptual framework on image watermarking which is widely used for security purpose within the epoch of data and Communication Technology. Image watermarking is predicated on the concept that the signal may carry several different watermarks at the identical time. The signal is also audio, pictures or video. Security issue in watermarking is because of enlargement of internet within the present paper the primary phase detailed description of watermarking has been on condition that data set are prepared on which watermarking technique are executed. In the second phase detailed working of the various techniques of image watermarking have to locate a selected watermarking technique which is able to provide appropriate ends up in term of PSNR and interval and various attacks are tested on images so implemented method must stand against various attacks. In third or final phase reverse process are executed to extract host and watermark image. There are many viable attacks. Spotting is an algorithm which is applied to the attacked signal to infusion the watermark from it. During this research paper, focused to increased the worth of PSNR because in existing techniques It's clear from the assessment that the proposed technique is long way stable than the prevailing technique.

Keywords— *Watermarking, Cover Image, Attacks, PSNR, DFT, DCT, Security*

1. INTRODUCTION

Watermarking is that the process of implanting data into a digital signal which can be accustomed support its authenticity or the identity of its owner. it's the thanks to protect multimedia files. a proof may sway several different watermarks at the identical time. In digital watermarking, the signal is also sound, icon or video. If the signal is simulated, then the data is additionally carried within the simulate. It allow users to engraft particular design or some information into digital contents without changing its perceptual quality. Watermarking may be a key process for the shelter of possession ownership of electronic information. There are many viable attacks.

Spotting is an set of rules which is applied to the attacked signal to infusion the watermark from it. If the signal wasn't changed during transmission, then the watermark continues to be present and it is evoked. The engrafting takes place by rigging the content of the digital data, which implies the information isn't engraft within the frame round the information. Inserting a digital data as an example images, audio, video, etc. with information and this digital data which can not be easily detach is understood as digital watermarking. With time more advanced technique came into domain of communication. Now every day to decrypt a cipher text is a straightforward task. Therefore have to design more robust technology, which may provide better security to our data as compared to cryptography and limitations of cryptography overcome by stenography and watermarking. The procedure within which information is hiding over a canopy image which informs can not be accessed by a 3rd party is understood as stenography. In watermarking concealed information is related to cover object, therefore we are able to say watermarking is sort of like steganography. Therefore watermarking technique used for copyright, preservation and holder authentication.

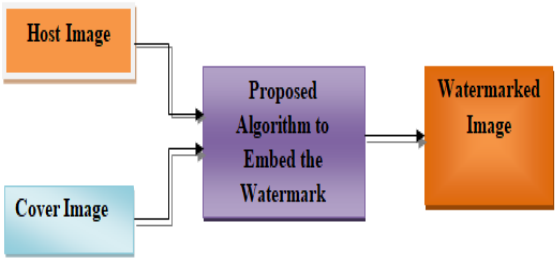

Fig.1: Basic Watermarking Principle

Types of watermark: There are mainly four styles of watermark:

(a) Robust watermark: a strong watermark may be a watermark that's difficult to get rid of from the thing during which it embedded.
(b) Fragile watermark: A fragile watermark is destroyed if anybody attempts to tamper with the thing during which it's embedded.
(c) Visible watermark: A visual watermark is instantly perceptible and clearly identifies the duvet object as copyright protected material.
(d) Invisible watermark: An invisible watermark isn't normally perceptible, but can still be employed by the rightful owner

as evidence of knowledge authenticity during a court of law.

Principle of Watermarking: There are mainly three different steps involved for a watermarking system:

- Embedding
- Attack
- Detection

In start which is embedding, host image and canopy image are accepted by an algorithm to get a watermarked image. Subsequently watermarked image or data is then communicated to a different person. When this person alters the communicated data, process in knowing as an attack and there are various attacks available which might be targeted at the information. Now in last step which is detected, to extract the watermark from attacking signal an algorithm is applied. During the communication process if the signal wasn't modified, then a watermark is yet present and it will be fetched. If the image is copied, then the information is additionally taken within the copy. The authentic image and appropriate watermark are inserted by implementing anyone technique out of assorted available to us. Now at the receiver side revoke process is executed to infusion watermark image from watermarked image. As there are various techniques available through which watermark inserted on the duvet image. during this process a secret secret's used for inserting and extracting for security reason that's why unauthorized people cannot access the information.

2. WORKING OF WATERMARKING

The working of watermarking is that it's the method of implanting information into a digital signal which can be accustomed assert its authenticity. In digital watermarking, the signal could also be sound, icon or video. If the signal is simulated, then the information is additionally gestated within the copy. Watermarking may be a key process for the possession of copyright ownership of electronic data. There are many viable attacks. Spotting is an algorithm which is applied to the assailed signal to aim to infusion the watermark from it. If the signal wasn't altered during contagion, then the watermark remains present and it will be extracted. The implanting takes place by manipulating the content of the digital information, which implies the information isn't implanted within the frame round the data.

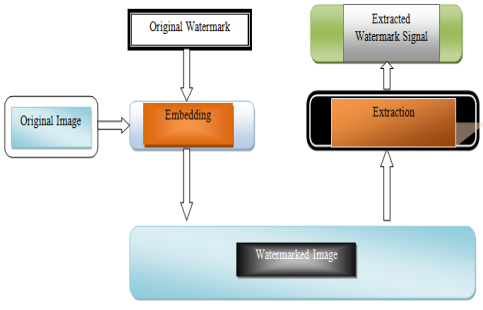

Fig.1: Block diagram of Watermarking

2.1 Merits

Some crucial edges of watermarking technique are listed below:

- **Keep Uniqueness:** Generally watermarking are often viewed as a copyright and it ends up in branding of a product as an example logo of TV channels, companies etc. It helps to locate genuine owner of a selected brand and depicts uniqueness of your product on the web site.
- **Copy Control:** Personal data uploaded on social networking website like Facebook, Instagram, twitter are often utilized by unauthorized person for illegal use and it represents a threat to piracy. Therefore Watermarking techniques help in protecting images. Out of invisible or visible, visible watermark are often added in digital image and pictures for safeguarding cognitive properties. Automatically scale your watermark image: it's necessary that watermarked image should always be smaller in size than the first image. The module for watermarking itself scales down proportional to image uploads with none image quality being lost. **Keep Authentic Image:** the first image are going to be kept by watermarking module in order that it are often downloaded at the time of requirement.
- **Mass Export and Import:** you'll import huge amount of knowledge with watermarked images and besides this export of giant data also possible in a very CSV file and keeping authentic image still because the original file name.

2.2 DEMERITS

As watermarking has such a big amount of advantages, but even have some limitations which are depicted below:

- If someone influences data or image, then watermarking disappear
- When any operation executed like compression, resizing form one kind of image to a different then watermark also reduced significantly.
- This technique unable to imitating images/ data, but help to locate ownership of imitating data/images.

3. DIGITAL WATERMARKING TECHNIQUE

Watermarking techniques are sorted out into two categories generally which are spatial domain techniques and frequency-domain techniques.

In spatial domain watermarking techniques, the hidden messages are directly engrafted into cover image. Here, the pixels in randomly selected regions of the photographs are qualified in keeping with the watermark chosen. There are three factors that find the parameters of the algorithm used during this technique. The three factors are the information related to the signature, the private random key, the masking property of a picture. the benefits of spatial domain methods are easy and easy implemented, high payload and supply a simple thanks to control. Least significant bit watermarking is an example of this type of technique. The limitation of this approach is that it's prone to every slight steganalysis method.

In frequency domain techniques like Discrete Wave Transform, Lifting Wavelet Transform, Discrete Cosine Transform, etc.., the duvet image converted into frequency domain coefficients before embedding the key message into it. a bonus of frequency domain techniques over spatial domain is that the ability for top resistance against steganalysis methods and signal processing manipulations. But transformations into frequency domain are basically computationally composite.

3.1 DFT

DFT is understood as RST (Rotation, Scaling and Translation) technique. There are various mathematical tools exist which are wont to transform a time domain signal into a frequency domain and Fourier transform is one in all them wont to transform the signal from the spatial domain to frequency domain. Discrete Fourier Transform i.e. DFT provide constructive diffusion of energy.

Merits

DFT is understood as RST (Rotation, Scaling and Translation) technique. Therefore DFT utilized for geometric distortion

Demerits

- To implement this can be a tedious task.
- It is additionally not economical.

3.2 DWT

By this system a picture is disintegrated into four different wavelets or segments. Out of those four segments one sub band are often selected as per our requirements and application then a watermark is inserted. Through this compression technique of image executed effectively. to help this there exists various filters like Symlets, Haar, Coiflets and Daubechies.

Merits

- It allows good localization both in spatial and time frequency domains
- Keep away blocking artifacts
- Compression ratios are excessive

Demerits

- DWT uses the larger DWT basis function
- This technique isn't economical
- Processing speed is low
- Also suffer from noise

3.3 LWT

Wavelet transforms decomposes data (image) into different spatial domain and independent frequencies and it's time domain analysis technique. When the image is DWT transformed, then the image is segmented into four regions which are HH, HL, LH and LL. Out of those, LL is low frequency segment and also the rest are high frequency segments. Figure 1 shows the one level Discrete Wave Transforms decomposition process. In DWT method blurring effect is generated by wavelet filter and this can be one in all the key drawbacks of DWT technique, together with some ringing noise produced at the perimeters of a picture. LWT overcomes this drawback of existed technique and besides this in the proposed technique time interval also minimized which is additionally a milestone.

Merits

- DWT limitations are overcome by LWT algorithm
- It reduces the computation time and speed up the computation process.

Demerits

It consists three segments: Splitting, prediction and updating therefore to implement is a smaller amount complex.

3.4 DCT

DCT could be a widely used transformation technique in signal processing and data compression.

Merits

- Unable to detach watermark thanks to embedding.
- In digital processing functioning DCT is more vigorous

Demerits

- When the quantization process executed some HF components conceal
- Unprotected against scaling and cropping

3.5 LSB

The LSB is that the bit position in a very binary integer giving the unit value,i.e. finding whether the amount is even or odd. Least Significant Bit is usually remarked because the RB i.e. rightmost bit, thanks to the established in number representation system of writing lower digits further to the proper.

Merits

- Simple to use and perceive
- Fair image class achieved.
- Utmost perceptual boldness.

Demerits

- Very sensitive to noise.
- Vulnerable to cropping, scaling attacks.
- Very less robust against attacks.

Table 1: Comparison of technique

Technique	Attack on Watermarked Image	LWT Robustness Level	DWT Robustness Level
DWT and LWT	Absence of attack	High	High
	Salt and Pepper Noise	High	Low
	De-blurred	High	Medium
	Resizing of scaled image	Medium	Low
	Scale to half size	Low	Low
	Rotation of 5 degree and rotated back	Low	Low
	Scaling to 75% of original size	High	High
	Cropping	Low	Low

From the above comparison it's clear that proposed technique is secure than the present technique.

5. APPLICATIONS

Watermarking technique utilized in diverse domain to secure the information. Some domains are listed as where this method used: copyright shielding, entertainment and data authentication, bioscience, defenseetc. A number of the applications are described below:

(a) **Copyright Protection**: To locate and preserve the copyright ownership, digital watermarking technique is used. Digital data is inserted together with watermarks portray metadata recognizing the copyright owners [2].

(b) **Medical application**: within the medical domain watermarking technique is extensively used. for instance digital watermarking used for printing crucial information like name, age, etc. of patient on MRI scan and X-ray reports. If this information isn't portray on X-ray and MRI scan and somehow reports mixed unintentionally then severe situation arises and causality is occurred.

(c) **Digital finger printing**: Fingerprint is that the characteristic of an entity which help to isolate it from other sorts of entity. In copyright protection applications watermark is employed for finger printing to locate genuine identity who breach license accord and dispense copyrighted data against the law.

(d) **Content archiving:** Generally digital data are identity by file names. Therefore this method is extremely delicate because file name is changed very easily. Therefore to

beat with this kind of scenario a object identifier is inserted in object. With this tampering possibility with data reduced.

(e) **Broadcast monitoring**: In broadcast monitoring watermarking technique is employed and it's an important use in profit oriented advertisement broadcasting. people who want to broadcast a advertisement want to understand whether advertisement was aired or not and if aired at right time and for what duration.

(f) **Tamper detection**: Digital data is identifying for tampering by inserting delicate watermarking. If there's degradation in delicate watermarking then it depicts that data is tried to change which data can not be trusted.

6. CONCLUSION

As the existing technique provide less security because of the less value of PSNR. to beat such quite the constraints within the present paper hybrid technique has been designed. the worth of PSNR just in case of existing technique is extremely less as compared to the proposed technique. There are various attacks exist like blur, average, crop and Gaussian which can destroy prime information from image but watermarked images stand against of these odds. within the present paper hybrid technique has been proposed to beat the protection issue of the present technique because of the low value of PSNR. it's going to be the concept of hybrid technique. In our research work Digital Image Watermarking administrated successfully using LWT, WHT and SVD. Blurring and ringing effect occur because of wavelet filter in DWT is overcome by proposed technique LWT which decomposes the image into different spatial domain and independent frequencies. Besides this one among the sting benefits of LWT computational time which is extremely fast. It provide high value of PSNR and also there's no possibility of any quite security attack which give very high level of security. Our proposed work is additionally robust to square against various sorts of attack like blur attack, motion attack and average attack. In our proposed technique, it's supported principle and mathematical expression and it shows result that our proposed technique provide more security than the present technique.

7. REFERENCES

[1] Mohamed Ali Hajjaji, Mohamed Gafsi, Abdessalem Ben Abdelali, Abdellatif mtibaa, "FPGA Implementation of Digital Images Watermarking System Based on Discrete Haar Wavelet Transform", Security and communication network, Volume 2019, 17 Pages, DOI: 10.1155/2019/1294267.

[2] Yuqi He, Yan Hu, "A Proposed Digital Image Watermarking Based on DWT-DCT-SVD", 2018 2nd IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC), 24 September 2018, 10.1109/IMCEC.2018.8469626

[3] Piyush Pandey, Rakesh Kumar Singh, "Novel Digital Image Watermarking Using LWT-WHT-SVD in YCbCr Color Space" International Journal of Innovative Research in Computer and Communication Engineering, Vol. 5, Issue 6, June 2017

[4] Varsha Purohit1 Bhupendra Verma2," A New Approach for Image Watermarking Using 3LWT-Walsh Transform-SVD in YCbCr Color Space " IJSRD - International Journal for Scientific Research & Development| Vol. 5, Issue 02, 2017

[5] Rajeev Dhanda and Dr. K. K Paliwal, "Hybrid Method For Image Watermarking Using 2 Level LWT-Walsh TransformSVD in YCbCr Color Space" International Journal on Recent and Innovation Trends in Computing and Communication Volume: 5 Issue: 11.

[6] Salma Hussainnaik, 2Farooq Indikar 3Reshma H Husennaik, "Review on Digital Watermarking Images" © 2017 IJEDR | Volume 5, Issue 2 | ISSN: 2321-9939.

[7] N.Vinay Kumar, Prof.A.Venkat Ramana, DR.C.Sunil Kumar and V.Raghavendra, "An Enhanced invisible Digital Watermarking Method for Image Authentication", International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 22 (2017) pp. 12016-1202.

[8] Mehdi Khalili and Mahsa Nazari, "Non Correlation DWT Based Watermarking Behavior in Different Color Spaces" (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, No. 1, 2016.

[9] Namita Chandrakar1 and Jaspal Bagga2, "Performance Analysis of DWT Based Digital Image Watermarking Using RGB Color Space" International Journal of Scientific Research Engineering & Technology (IJSRET), ISSN 2278 – 0882 Volume 4, Issue 1, January 2015.

[10] D.Vaishnavia, T.S.Subashinib, "Robust and Invisible Image Watermarking in RGB Color space using SVD" International Conference on Information and Communication Technologies (ICICT 2014).

[11] Amit Kumar Singh, Mayank Dave and Anand Mohan, "Hybrid Technique for Robust and Imperceptible Image Watermarking in DWT–DCT–SVD Domain" The National Academy of Sciences, pp. 351–358 India 2014, 19 July 2014

[12] Pravin M. Pithiya and H.L.Desai, "DCT Based Digital Image Watermarking, Dewatermarking & Authentication" International Journal of Latest Trends in Engineering and Technology (IJLTET), Vol. 2 Issue 3 May 2013.

[13] Dr. H. B. Kekre, Dr. Tanuja Sarode and Shachi Natu, "Performance Comparison of DCT and Walsh Transforms for Watermarking using DWT-SVD" (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 4, No. 2, 2013.

[14] Anuradha, Rudresh Pratap Singh, "DWT Based Watermarking Algorithm using Haar Wavelet," International Journal of Electronics and Computer Science Engineering, Vol. 1, No. 1, 2012.

[15] Rahim Ansari, Mrutyunjaya M Devanalamath, K. Manikantan and S. Ramachandran, "Robust Digital Image Watermarking Algorithm in DWT-DFT-SVD Domain for Color Images" 2012 International Conference on Communication, Information & Computing Technology (ICCICT), Oct. 19-20, Mumbai, India

[16] Huang–Chi Chen, Yu–Wen Chang, Rey–Chue Hwang, "A Watermarking Technique based on the Frequency Domain," Journal of Multimedia, Vol. 7, No. 1, 2012

[17] Anjul Singh Akash Tayal , "Choice of Wavelet from Wavelet Families for DWTDCT-SVD Image Watermarking" International Journal of Computer Applications (0975 – 888) Volume 48– No.17, June 2012.

[18] Ante Poljicak, Lidija Mandic, Darko Agic, "Discrete Fourier transform–based watermarking method with an optimal implementataion radius," Jounal of electronic imaging, 2011

[19] Mehdi Khalili 1 and David Asatryan, "Effective Digital Image Watermarking in YCbCr Color Space Accompanied by Presenting a Novel Technique Using DWT" Institute for Informatics and Automation Problems of NAS of RA,

Mathematical Problems of Computer Science 33, 150—161, 2010

[20] V. Santhi and Arunkumar Thangavelu, "DWT-SVD Combined Full Band Robust Watermarking Technique for Color Images in YUV Color Space" International Journal of Computer Theory and Engineering, Vol. 1, No. 4, October 2009 , 1793-8201

[21] Zhicheng Ni, Yun-Qing Shi, Nirwan Ansari, and Wei Su, "Reversible Data Hiding" IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 16, NO. 3, MARCH 2006

[22] Mauro Barni, Member, IEEE, Franco Bartolini, Member, IEEE, and Alessandro Piva, "Improved Wavelet-Based Watermarking Through Pixel-Wise Masking", IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 10, NO. 5, MAY 2001

[23] Sviatolsav Voloshynovskiy, Shelby Pereira, and Thierry Pun, "Attacks on Digital Watermarks: Classification, Estimation-Based Attacks, and Benchmarks" IEEE Communications Magazine • August 2001

[24] Ming-Shing Hsieh, Din Chang Tseng and Yong-Huai Huang, "Hiding digital watermarks using multiresolution wavelet transform", IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, VOL. 48, NO. 5, OCTOBER 2001

[25] Chiou-Ting Hsu and Ja-Ling Wu , "Multiresolution Watermarking for Digital Images" IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS—II: ANALOG AND DIGITAL SIGNAL PROCESSING, VOL. 45, NO. 8, AUGUST 1998.

[26] Mauro Barni, Franco Bartolini, Vito Cappellini, Alessandro Piva, "A DCT-domain system for robust image watermarking" M. Barni et al. / Signal Processing 66 (1998) 357–372.

[27] J.J.K.0 Ruanaidh W.J.Dowling F.M. Boland, "Watermarking digital images for copyright protection" IEE ProcVis. Image Signal Process., Vol. 143, No. 4, August 1996.

[28] Awanish Kr Kaushik, "A Novel Approach for Digital Watermarking of an Image Using DFT," IJECSE, Vol. 1, No. 1, pp. 35–41, 2012

[29] Pallavi Patel, D. S. Bormane, "DWT Based Invisible Watermarking Technique for Digital Images," International Journal of Engineering and Advanced Technology, Vol. 2, No. 4, 2013

[30] Chih–Chin Lai, Cheng–Chih Tsai, "Digital Image Watermarking using Discrete Wavelet Transform and Singular Value Decomposition," IEEE Transactions on Instrumentation and Measurement, Vol. 59, No. 11, 2010.

[31] Advith J, Varun K R and Manikantan K, "Novel Digital Image Watermarking Using DWT-DFT-SVD in YCbCr Color Space" International Conference on Emerging Trends in Engineering, Technology and Science (ICETETS), 24-26 Feb 2016, **DOI:** 10.1109/ICETETS.2016.7603032

