A Review on Digital Image Watermarking with its Techniques and Properties

Varsha Purohit[1], Bhupendra Verma[2]
[1, 2] Department of Digital Communication
[1, 2] NITM Datiya, India

Abstract- *Digital watermarking (DW) of multimedia content has become a very energetic studies location during the last several years. Watermarking is a totally critical subject for copyrights of numerous digital files and media. With pictures widely available on the Internet, it could occasionally be ideal to use watermarks. DW is the processing of blended statistics into a digital signal. A watermark is a secondary image, which is overlaid on the host image, and offers a way of protective the photograph. The DW technique could be very astounding for picture authentication or safety for attacks. In this paper, we goal to provide a survey of various varieties of digital watermarks and techniques to do image watermarking. Problems and challenges to produce watermarked images are also analyzed and reported. Given in the document for the papers to be published. You can use this record as both a preparation set and as a template into which you may types your personal textual content.*

Keywords- Digital Image Watermarking(DIW);Spatial Domain Techniques(SDT);LSB(Least significant bits); Frequency Domain Technique (FDT); DCT (Discrete Cosine Transform) ; DWT(Discrete Wavelet Transform)

I. INTRODUCTION

Digital watermarking (DW) is the embedding or hiding of statistics inside a digital file without fairly changing the document itself. Now DIW is growing attention because of the quick growing in the internet visitors. DW executed is popularity due to its significance in content authentication and copyright safety for digital multimedia information. [1]. Various DW techniques are purposed for copyright safety of multimedia facts from being misused. Watermarking is the technique of embedding facts right into a multimedia element which include a picture, audio or video record for the reason of authentication. This embedded information may be later extracted or detected the multimedia facts for safety functions. A watermark is a statistics approximately foundation, possession and copy manage. This fact is embedded in multimedia content with taking care of imperceptibility and robustness. General block diagram of watermarking is shown in Fig.1

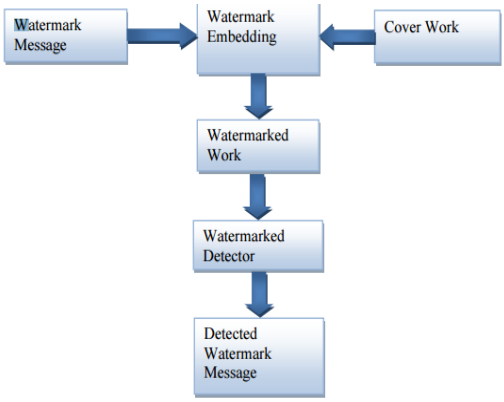

Figure 1. Fig. 1. The Watermarked Embedding and Detection Process

According to the embedding area of the host picture, DIW can be categorized into one of the two domain names via spatial and remodel. The easy method within the SDT is to insert the watermark image (WI) pixels in the LSB of the host picture pixels. In the ability of records, hiding is high in those techniques however hardly robust. Watermarking inside the transform area is more at ease and robust to numerous attacks. In Frequency area, the watermark isn't always added to the picture intensities or pixels, however to the values of its transform coefficients. Then to get the WI, one has to carry out the remodel inversely. It includes DCT (Discrete Cosine Transform), DFT (Discrete Fourier Transform), and DWT (Discrete Wavelet Transform).[1]

1. Types of digital watermark

1) Visible digital watermark(VDW):

A visible watermark is a visible semi-transparent text or image that is laid on the host image. It permits the host picture to be considered, but it still affords copyright protection by way of marking the photograph as its owner’s assets. Visible watermarks are stronger against picture transformation. Thus they're preferred for strong copyright safety of highbrow property that’s in digital format. A visible watermark in reality identifies the quilt item as copyright-protected [2].

2) Invisible watermark (IW):

An IW is an embedded picture which cannot be visible with human's eyes. Only digital devices or specialized software can extract the hidden facts to discover the copyright proprietor. IW is used to mark a specialized digital content (textual content, picture or maybe audio content material) to show its authenticity.

3) Fragile watermark (FW):

An FW is destroyed if every person attempts to tamper with the object in which it is embedded. A DW is referred to as fragile if it turns into fail to be detectable after the slight modification. FW are typically used for tamper detection (integrity evidence). Modifications to an authentic work that virtually are substantial and commonly aren't known as watermarks however as generalized barcodes.

4) Robust watermark (RW):

A DW is known as strong if it resists any sort of changes. RW may be used in replica safety applications to hold the copy and no access manipulate records. It is hard to cast off from the item wherein it's far embedded. These watermarks can't be damaged easily. RW should remain intact permanently in the cover image (CI). If we try to remove robust watermark then quality of image will be degraded.

2. Process of Image Watermarking

The system of watermarking is divided into 2 parts:

a) Embedding of the watermark into the host picture.
b) Extraction of the watermark from the picture.

A. Watermarking Embedding

The procedure of picture watermarking is complete at the source finish. In this process watermark is embedding in the host Image by using any watermarking algorithm or process. The whole process is shown in figure 2

When it comes to the planning which is the prominent step in the industry it helps in the defining the needs and the objectives and functional causes of the systems and supporting technologies, the planning is done by the consultants and the developers in the team association with the plant management and engineering and finance and operation departments. In order to improve the operational efficiency, the material handling it should be deployed with sturdy consistency and predictability.

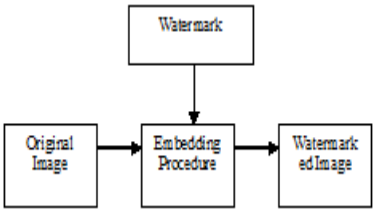

Figure 2. Embedding process of image watermarking

B. Watermarking Extraction

This is the process of Extracting watermark (EW) from the WI by way of reverse the embedding algorithm. The entire procedure is shown in fig. 3

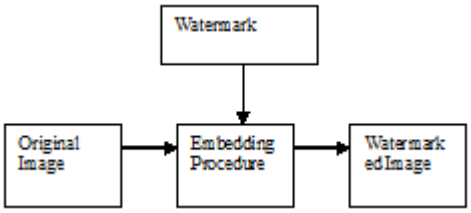

Figure 3. Extraction process of image watermarking

3. Watermarking Properties

Watermarking desires a few suitable properties based on the software of the watermarking device [3]. Some of the homes are supplied right here:

a) Effectiveness:

This is the most significant property of watermark that the watermark must be powerful manner it must without a doubt be the detective. If this may now not take place the aim of the watermarking isn't always fulfilled.

b) Host signal Quality:

This is also an important asset of watermarking. Everybody is aware of that in watermarking; the watermark is embedded in host sign (image, video, audio and so forth.). This may put an effect at the host sign. So the watermarking device needs to be like because it will minimal modifications the host signal and it ought to be unnoticeable whilst the watermark is invisible.

c) Watermark Size

Watermark is regularly used to owner identification or security confirmation of host sign and it usually uses when statistics is transmitted. So it is important that the size of watermark should be minimum because it will increases the size of data to be transmitted.

d) Robustness

Robustness is the vital assets for all watermarking systems. There are so many reasons by way of which watermark is degraded, altered at some stage in transmission, attacked by way of hackers in paid media programs. So watermark must strong So that it withstands all of the assaults and threats.

Applications of Digital Watermarking

1. Owner Identification: It establishes possession of the content.
2. Copy Protection: It prevents human beings from making unlawful copies of copyright content.
3. Authentication of Content: To detect modifications of the content as a sign of invalid authentication.
4. Fingerprinting: Trace back illegal copying and copying of the content.
5. Broadcast Monitoring: Specially for commercials and in leisure industries, to display content material this is broadcast as shriveled and through the authorized supply.
6. Medical Applications: Used to provide both authentication and confidentiality without affecting the medical image in any way.[4]

Objectives

The main objectives of this research are:

i. To implement a watermarking scheme using repetition codes (3, 1) in DCT.
ii. To test the watermarked scheme towards commonplace attacks like salt and pepper, speckle, compress, Gaussian, picture contrast, resizing and cropping attacks.
iii. To estimate the robustness of the system by general metrics like Mean Squared Error (MSE), Peak Signal-To-Noise Ratio (PSNR) and Normalized Correlations (NC).

II. LITERATURE REVIEW

[5] This paper gives DW for their applications, techniques, attacks, classifications and tampering detection. With the help of those techniques, they enhance the security of picture. This paper worked on RGB components which include red, green, blue for boosting robustness and security. 2-DWT applied on RGB components for desirable effects. The author concluded that tampering detection and watermarking method may be very critical for protection towards attacks.

[6] Introduced a block based picture watermarking algorithm which makes use of the cryptographic algorithm to discover the location of the CI in which watermark is to be embedded. The one of a kind keys are generated the use of Diffie Hellman Key Exchange Algorithm and using those keys the location of CI to which the watermark are to be embedded are discovered out. The embedding is done after block dividing the CI and WI. The experimental consequences show that the proposed approach is strong.

[7] In this paper a modern digital video watermarking scheme is proposed which mixes DWT and Singular Value Decomposition (SVD) in which watermarking is carried out within the high-frequency sub band after which numerous varieties of assaults had been implemented. The watermark object has been embedded in every body of the unique video. Since in each body, the watermark is embedded and it affords robustness towards assaults.

[8] Introduced a at ease and sturdy watermarking algorithm based totally on the mixture of picture interlacing, DWT & DCT techniques. After the formation of WI. Secondly, Error correcting codes are used to reduce noise over the channel by correcting and detecting errors. The uncompressed image needs more storage and bandwidth than compressed image. With EBCOT (Embedded block coding optimal truncation) algorithm image compression is done effectively.

[9] This paper provides comprehensive survey on various DIW techniques in different domains and their requirements. The author introduced the survey and classified the different requirements, benefits and limitations. It has been concluded that to limit distortions and to growth potential, strategies in frequency domain have to be blended with another approach which has strong robustness and excessive capability in opposition to dissimilar types of attacks.

[10], In this paper a new approach is proposed the use of the aggregate of DCT and PCA rework which will reduce the low-frequency band for the color picture in YUV color area. The Y (luminance) is divided into non-overlapping blocks and the low band coefficients of every block are placed inside the matrix data than PCA remodel are applied to it. This method eliminates the disadvantage of low band based on the combination of DCT and PCA transform.

[11] Introduce two methods for invisible and robust watermarking proposed in RGB color space. In the first approach, the grayscale watermark is embedded within the blue coloration channel and in the 2nd method; blue shade watermark is embedded within the blue color channel element

and then SVD carried out at the blue channel of host picture to retrieve singular values. They concluded that the primary approach gives an excellent robustness for median filtering assaults, for motion blur and so forth. And the second approach offers true robustness for Gaussian noise, salt-pepper noise and so forth.

[12] Authors have introduced a comfy and sturdy record hiding the set of rules primarily based on hiding in random coefficient of DWT and scholar t-distribution. Performance evaluation of imperceptibility and robustness of proposed set of rules has been made the usage of PSNR and Bit Error Rate (BER) price for one of a kind watermark and pictures which include Lena, Gibbon, and Fruit pictures. The result achieves higher security and robustness against jpeg compression as well as many attacks such as rotation, cropping etc.

[13] In this paper authors have combined the strategy of Steganography, DW and cryptography using DCT, DWT and SVD algorithm which provide security of images properly as the authenticity of the picture. DWT altered 2-D picture into 4 sub-bands i.e. Low-Low(LL),High-Low(HL),Low-High(LH),High-High(HH). The LL sub band again split into those 4 sub-bands and this technique is called 2DWT. Authors more desirable their research by encrypting image statistics the usage of RSA set of rules.

[14], In this paper, divide the host image into four overlapping square segments called sub-picture and the watermark is independently embedded into each of them, using hybrid scheme. The redundancy reduces the effect of cropping image. Authors proposed a synchronization technique to recover geometrically attacked image via. Detection of desired image corner.

III. DIGITAL WATERMARKING TECHNQUES

The various watermarking techniques are:

1. Spatial Domain Techniques:

Spatial domain watermarking (SDW) tiny modifies the pixels of 1 or randomly decided on subsets of a picture. However, this technique isn't always reliable even as subjected to regular media operations inclusive of filtering or lossy compression. Various spatial location techniques are as follows [3]:

a) Least Significant Bit Coding (LSB):

LSB coding is one of the earliest techniques. LSB may be done in any shape of watermarking. In this approach, the LSB of the service sign is substituted with the watermark. The bits are embedded in a series which acts as the important thing. In order to retrieve its lower back, this series ought to be acknowledged. It then embeds the facts on the LSBs of the pixels from this subset. LSB coding is a totally easy technique but the robustness of the watermark may be too low. With LSB coding almost usually the watermark cannot be retrieved without a noise aspect.

b) Predictive Coding Schemes:

In this technique, the correlation among adjoining pixels is exploited. A set of pixels in which the watermark must be embedded is selected and exchange pixels are changed by means of the difference between the adjacent pixels. This may be similarly improved by adding a regular to all the differences. A cipher secret is created which permits the retrieval of the embedded watermark on the receiver. This is an awful lot extra sturdy as compared to LSB coding.

c) Correlation-Based Techniques:

In this method, a pseudo-random noise (PN) with a sample W(x,y) is brought to a photo. At the decoder, the correlation between the random noise and the picture is located out and if the value exceeds a certain threshold cost the watermark is detected also it isn't.

d) Patchwork Techniques:

In patchwork watermarking, the image is split into 2 subsets. One feature or an operation is chosen and it is applied to these two subsets in the opposite direction. For instance if one subset is increased by a factor k, the other subset will be decreased by the same amount.

2. Frequency Domain Techniques:

The frequency Domain (FD) is that in which the secret information are hidden within the lowest or center frequency portions in covered photo, because of the higher frequency portion is extra be suppressed by compression. It is important and difficult that how to select the best frequency portions of the picture for watermark. There are various FD techniques that are as follows:

a. Discrete Cosine Transform (DCT) based Technique:

It is a system that is converts a series of information factors within the SD to a sum of sine and cosine waveforms

with exclusive amplitudes inside the FD. The DCT is a linear remodel, which maps an n-dimensional vector to a set of n coefficients. It may be very strong to JPEG compression, on account that JPEG compression itself makes use of DCT.

b. Discrete Fourier Transformation based technique:

It is translation invariant and rotation resistant, which interprets to sturdy robustness to geometric attackss. DFT uses complex numbers, while DCT uses just real numbers.

Discrete Wavelet Transform based Technique:

DWT primarily based strategies allow good spatial localization and have a multi-resolution significance that is equal to the human visual gadget. This approach also shows the robustness to low pass & median filtering. But, these are not robust to geometric transformations.

3. Wavelet Transform based Watermarking:

The WT primarily based watermarking technique divides the photograph into four sidebands a low-decision approximation of the tile factor and the thing's horizontal, vertical and diagonal frequency tendencies. The system can then be repeated iteratively to supply N scale remodel [15].

Table 1. Comparisons Of Different Watermarking Techniques

Algorithm	Advantages	Disadvantages
LSB	1. Easy to implement and understand 2. Low degradation of image quality 3. High perceptual transparency.	1. It lacks basic robustness 2. Vulnerable to noise 3. Vulnerable to cropping, scaling.
Correlation	1. Gain factor can be	1. Image quality gets
	increased resulting in increased robustness	decreased due to very high increase in gain factor.
Patchwork	1. High level of robustness against most type of attacks	1. It can hide only a very small amount of information.
Texture mapping coding	1. This method hides data within the continuous random texture patterns of a picture.	1. This algorithm is only suitable for those areas with large number of arbitrary texture images.
DCT	1. The watermark is embedded into the coefficients of the middle frequency, so the visibility of image will not get affected and the watermark will not be removed by any kind of attack.	1. Block wise DCT destroys the invariance properties of the system. 2. Certain higher frequency components tend to be suppressed during the quantization step.
DWT	1. Allows good localization both in time and spatial frequency domain 2. Higher compression ratio which is relevant to human perception.	1. Cost of computing may be higher. 2. Longer compression time. 3. Noise/blur near edges of images or video frames.
DFT	1. DFT is rotation, scaling and translation (RST) invariant. Hence it can be used to recover from geometric distortions	1. Complex implementation 2. Cost of computing may be higher.

IV. CONCLUSION

The Digital Image Watermarking is progressing very speedy and various researchers from numerous fields are focusing on broadening robust watermarking schemes. This paper reviewed the research work accomplished on DIW. It provided the primary version for embedding and extraction of the watermark. Next, it referred to the characteristic of the watermarking system. Then it listed a number of the programs of DIW. Finally, the possible attacks on DIW are mentioned.

REFERENCES

[1] Komal Tomar, "A Review Paper of Different Techniques on Digital Image Watermarking Scheme for Robustness". 2015, IJARCSSE

[2] Er. Sonia, Er. Naresh Kumar Garg, Er. Gurvinder Singh, "A Survey on Digital Image watermarking". 2014 IJARCET

[3] Lalit Kumar Saini, Vishal Shrivastava, "A Survey of Digital Watermarking Techniques and its Applications". (IJCST) 2014

[4] Deepti Shukla, Nirupama Tiwari and Deepika Dubey, "Survey on Digital Watermarking Techniques".ijsip 2016 SERSC

[5] Madhuri Rajawat, D S Tomar,"A Secure Watermarking and Tampering detection technique on RGB Image using 2 Level DWT", proc. IEEE 2015.

[6] Aparna J R, Sonal Ayyappan,"Image Watermarking using Diffie Hellman Key Exchange Algorithm", proceeding of the International Conference on Information and Communication Technologies(ICICT), pp:1684-1691, 2015.

[7] Divjot Kaur Thind, Sonika Jindal," A Semi Blind DWT-SVD Video Watermarking", pp:1661-1667, 2015.

[8] Ms. Mahejabi Khan, Mr. Ajay Kushwaha, Mr. Toran Verma,"A new digital image watermarking algorithm based on image interlacing,DWT,DCT", IEEE (ICIC) college of Engineering Pune,India. May 28-30,2015, pp:885-890.

[9] Urvi H.Panchal, Rohit Srivastava,"A Comprehensive Survey on Digital Image Watermarking Techniques", IEEE , 2015.

[10] Arash Saboori, S. Abolfazl Hosseini,"Color Image Watermarking in YUV Color Space Based on Combination of DCT and PCA", IEEE 23rd Iranian Conference on Electrical Engineering(ICEE), pp:308-313, 2015.

[11] D. Vaishnavi, T.S.Subashini,"Robust and Invisible Image Watermarking in RGB Color Space using SVD", procedia computer science 46, International Conference Information and Communication Technology(ICICT), pp:1770-1777, 2015.

[12] Surbhi Singh, Harsh Vikram Singh, Anand Mohan,"Secure and Robust Watermarking Using Wavelet Transform and student t-distribution", procedia computer science 70, 4th International Conference on Eco-friendly Computing and Communication System(ICECCS), pp:442-447, 2015.

[13] Palak Patel, Yash Patel,"Secure and authentic DCT image steganography through DWT-SVD based Digital watermarking with RSA encryption", IEEE , 2015.

[14] Saeid Fazli, Masoumeh Moeini,"A robust image watermarking method on DWT,DCTand SVD using a new technique for correction of main geometric attacks", Optik 127, Elsevier, pp:964-972, 2016.

[15] Manjinder Kaur and Varinder Kaur Attri, "A Survey on Digital Image Watermarking and Its Techniques".ijsip 2015

[16] Prabhishek Singh, R S Chadha, "A Survey of Digital Watermarking Techniques, Applications and Attacks". (IJEIT) 2013