MULTIPLE IMAGE WATERMARKING APPROACH BASED ON ANFIS FOR COPYRIGHT PROTECTION AND IMAGE AUTHENTICATION: A Review

Anmol Awasthi, M.Tech Scholar, Department of Computer Science & Engineering, Vishveshwarya Group of Institutions, Gautam Buddh Nagar, India.
Madhu Lata Nirmal, Assistant Professor, Department of Computer Science & Engineering, Vishveshwarya Group of Institutions, Gautam Buddh Nagar, India.

Abstract—. The watermark should be durable and undetectable. Watermark robustness can be explained in terms of successful watermark restoration from recovered relevant content that may also contain various forms of sounds and compression effects. The process of digital image watermarking is exact in that it inserts digital data into a digital signal. Watermarking is a technique for embedding records into virtual materials such as text, still photos, video, and audio statistics without affecting the overall quality of the digital media. is a green technique to avoid unauthorised statistics copying from multimedia networks. Watermarking is a widely used copyright protection and authentication tool. This paper gives an overview of the many theories and research projects in the field of image watermark authentication.

The patchwork signal and a watermarked sign The host signal is the signal in which the watermark will be placed. The three wonderful steps of a watermarking device are embedding, attack, and detection. The host and the data to be embedded are accepted by a series of rules, which results in a watermarked signal.

Digital watermarking is the process of embedding records, also known as digital signatures or watermarking, within a digital signature in a way that makes them difficult to remove. Virtual watermarks can be used to validate the service signal's legitimacy or integrity, as well as to reveal the owners' identities.

***Keywords*—** Digital Image Watermarking, DWT, PSNR, MSE.

I. INTRODUCTION

A digital watermark is a type of marking that includes audio, video, or photo information and is hidden within a noise-tolerant sign. The information to be embedded in a sign is referred to as a digital watermark, despite the fact that the term digital watermark is used to differentiate between traditional watermarks in some contexts. Virtual watermarks are only visible in positive situations. A watermark attack is a type of virtual information attack in which an attacker may identify the existence of a specially created piece of data without knowing the encryption key. The type of assaults should be given special attention because they can aid in the development of improved watermarking tactics and the definition of better standards.

For dealing with unique packages, a variety of watermarking strategies have been proposed. Some examples include:

1. Copyright-related programmes with a heavy integrated watermark
2. Watermarks that are generally fragile or semi-fragile in clinical, forensic, intelligence, or military programmes
3. In content authentication methods where even minor changes to the content material are unsuitable, flawless embedding distortion compensation is required.

Spatial watermarking techniques and spectral watermarking methods are two types of watermarking algorithms. Watermarking in the spatial area is a low-stage encoding that comprises the most basic processes such as side detection, shade separation, and so on. The set of criteria for spectral area watermarking is very complicated, yet it can be quite effective

against sign processing attacks. Discrete wavelet transform (DWT), discrete cosine transform (DCT), and discrete Fourier Transform (DFT) are spectral domain reconstruction techniques.

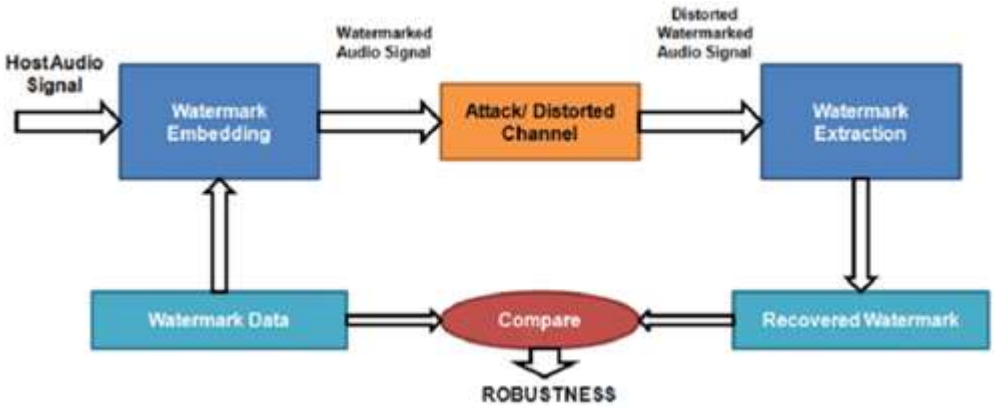

Figure 1: Watermarking System [12]

II. Related Work

Up to anticipated sitting then extraction on the watermark inside the grayscale image is proven to be less difficult than vile really modify procedures, according to Akhil Pratap Singh and Agya Mishra (2011). They describe the digital watermarking technique for digital images based on the International Journal of Scientific Research in Science, Engineering, and Technology (ijsrset.com) 931 toughness distinct wavelet significantly alter by assessing a number of PSNR's and MSE[1].

MSE, PSNR, BER, Malika Narang, and Sharda Vashisth (2013) all support watermarking based on DWT (discrete wavelet transform) milling between transform domains. Watermarking algorithms have been debunked by a few of companies based entirely on extraction: Watermarking that is both blind and non-blind. Original image is no longer required for unsuitable watermarking extraction, however original photos is required for non-blind watermarking extraction. He employs non-blind watermarking in it bill [9].

The system for digital watermarking was designed by Anum Javeed Zargar or Ninni Singh (2014), who used Discrete wavelet transformation but the wave filter we have is HAAR wavelet. This law also establishes the watermark's resilience when applied to a digital image. This is especially important with weak watermarking, as most of it can be readily removed during the basic photo modification. In some cases, the imperceptibility of a watermark prevents it from being used for nefarious purposes [3].

Dr. V V Nath (2016) and Ravi K Sheth (2016) both recommended a safe digital watermarking technology that can be used indefinitely for information validation. This procedure is both safe and effective. Because they bear aged combination over separate cosine transform (DCT) then by wavelet transform (DWT) tactics with cryptographic approach, the protected digital watermark is supplied by a hybrid way (Arnold Transform). This method provides high resilience and perceived transparency in accordance with the watermarked photo and unique photo against attacks such as cropping, uproar, and scaling. They discovered that the DCT-DWT technique outperforms the LSB and DCT strategies in terms of conformance [11]. As a result, the proposed method over DCT-DWT provides more desirable resilience and appreciating transparency in accordance with the watermarked image than unique picture against one-of-a-kind variety of attacks such as noise, cropping, or scaling.

Hina Lala (2017) devised a digital picture watermarking technique based on unique wavelets, which significantly altered the use of alpha blending. This approach incorporates a visible watermark into the cowl image. The extraction technique necessitates the use of the cowl image. The benefit of a tranquil watermark photograph and a watermarked image is dependent on the scaling factors, thus q [6].

III. DIGITAL WATERMARKING TECHNIQUE LEVEL

Watermarking methods for digital images can be classified in a variety of ways.

2.1 Stability

2.2 Perceptibility

2.3 Abilities

Stability: If the encoded statistics can be consistently detected from the marked sign, a digital watermark is said to be durable in terms of transformations. A virtual watermark is "fragile" if it becomes undetectable even after minor changes. It is commonly used to detect tampering (integrity evidence). If a virtual watermark resists benign changes but fails to be detected after malignant changes, it is said to be semi-fragile. Its miles are commonly utilised to detect cancerous differences. In copy protection software, strong watermarks can be used to carry reproduction and no access modify statistics. As a result, the watermark does not degrade after a few assaults and can be easily spotted to offer certification. [10].

Perceptibility : On films and photographs, a virtual watermark is characterised as perceptible if its presence in the marked signal is significant. Some are made transparent/translucent for user convenience attributed to the reason that they block part of the view, so diminishing it.

Abilities: It can be defined as the number of information bits encoded by a watermark in a unit of time or labour. Watermarks must be able to provide enough information to establish the image's uniqueness.

IV. A METHOD TO DIGITAL WATERMARKING

Watermarking is the process of putting a watermark in a multimedia object. A watermark can be thought of as a type of signature that identifies the owner of a multimedia object. A set of rules for watermarking embeds a visible or invisible watermark in a multimedia product. The embedding technique is led by the use of a secret key that determines where the watermark can be put into the multimedia item (picture). The entire digital image watermarking method operates in domain names, both geographical and rework areas, all of the time. In the rework domain, a photograph is represented by frequencies, whereas in the spatial domain, miles are represented by pixels.

Techniques for Watermarking a Spatial Area

The basic facts are loaded into the legitimate photo using spatial area virtual watermarking techniques at the same time. It's also possible to do it with colour separation. Watermarking in the spatial region is easier and faster than in the remodel area, but it is less resistant to attacks.

Additive watermarking: It is by far the most straightforward technique for embedding the watermark in the spatial domain. It's done by adding a pseudo-random noise sample to the depth of the image pixels.

Least significant bit: Watermarking is accomplished by selecting a subset of photo pixels and replacing the LSB of each of those pixels with watermark bits. Using this method, the watermark is embedded into the LSB of pixels.

- Simplicity
- Very low computing complexity;
- consuming takes much less time.

Approaches for Watermarking Frequency Areas

The watermark is inserted into the spectral coefficient of the image in the frequency area. The discrete cosine rework (DCT), discrete Fourier transform (DFT), and discrete wavelet rework are the most commonly used methods in the frequency domain (DWT).

DCT area watermarking: When compared to simple spatial area watermarking tactics, DCT based fully watermarking strategies are more resilient. DCT, like a Fourier transform, represents data in terms of frequency space rather than amplitude space. International DCT watermarking and block-based DCT watermarking are two types of DCT domain watermarking.

Steps in the DCT block are essentially based on a set of watermarking criteria.

1. Divide the image into 8x8 non-overlapping parts.
2. Perform a DCT on each of those blocks ahead of time.
3. Put some block choice standards to the test (e.g. HVS)
4. Stick to the coefficient selection criteria (e.g. maximum)
5. Enhance the specified coefficients to embed a watermark.
6. Check each block for inverted DCT rework.

DWT domain watermarking: DWT-based watermarking methods use the same pointers as DCT-based watermarking schemes, i.e. the underlying concept is the same; but, the system used to transform the photo into its transform area differs, and the resulting coefficients are unique. The photo is converted using wavelet filters in wavelet transforms.

Because it encourages time-frequency sign decompositions, discrete wavelet rework (DWT) is commonly used in image processing software. A sign can be split into distinct sub-frequency bands using DWT. To breakdown the signal into particular ranges, DWT employs each low pass clean out and excessive skip filter.

At every degree of decomposition, the significance of dwt coefficients is bigger in the lowest bands and smaller in the other bands (HH, LH, and HL). [13] [8]

Watermarking in the DFT domain: The DFT domain has been researched because it is resistant to geometric assaults such as rotation, scaling, cropping, and translation. In this chapter, we'll look at some DFT-based watermarking methods.

DFT of a real image is usually complex valued, thus DFT demonstrates translation invariance. The section illustration of the photo is influenced by spatial variations within the image, but not the importance representation [8].

DFT is also resistant to cropping since the impact of cropping results in spectrum blurring. When you scale in the spatial domain, you get inverse scaling in the frequency domain. The equal rotation within the frequency area is caused by rotation within the spatial area.

Lifted Wavelet Transformation (LWT) for Image creates a multi-resolution image representation. When it comes to deciphering visual data, a multi-resolution artwork provides a straightforward hierarchical mould. The main points of a Photograph normally represent unique physical buildings within the image at one-of-a-kind resolutions. This little print corresponds to the large buildings that give the image content at a medium stage resolution. The LWT and ILWT steps of the wavelet transform correlate to two critical steps (Inverse LWT). LWT divides a digital signal into two quadrants: the exorbitant frequency foot and the mangy frequency quadrant. The ragged frequency quarter is split up again, this time with a few more pieces on excessive or ignoble frequencies, and the process is continued until the sign is completely deconstructed. Decompositions of 1-5 degrees are commonly employed in watermarking. ILWT is used to render the reconstruct on the unique signal beyond the deconstructed photo. Because of decomposition, several types of wavelets exist. In general, LWT software separates an image into four tributary catena (Figure 2a), which derive from separate vertical and horizontal factors. The evident applications of the images are represented by the LH, HL, and HH tributary catenas, while the approximation over the image is represented by the LL under strip. The LL sub-band is additionally decomposed to reach the next underhand level (Figure 2c), culminating in the 2-level wavelet decomposition. The software determines the level of breakdown rendered. The current study addresses the above-mentioned breakdown in terms of pair levels [13].

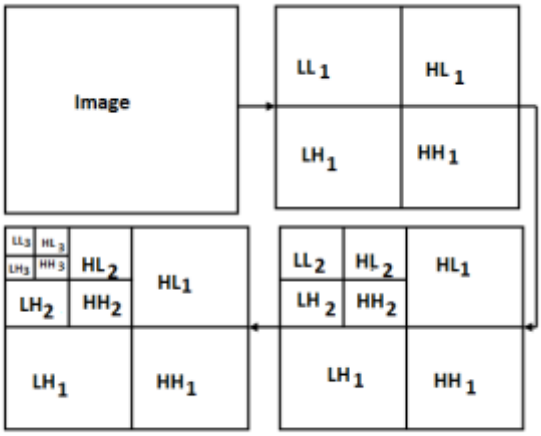

Figure 2: 3-Level LWT Decomposition

V. ANALYSIS OF DIFFERENT WATERMARKING TECHNIQUES IN COMPARISON

Table 1 shows a comparison of the benefits and drawbacks of various watermarking techniques. [3]

Algorithm	Advantage	Disadvantage
DCT	1. Extremely resistant to activities involving digital processing. 2. Because of the embedding, no attempts can remove the watermark. Incorporate a watermark into the middle frequency coefficient.	1. Even during quantization process, certain higher frequency components are suppressed. 2. Block wise DCT undermines the system's invariance features. .
DWT	1. Increased compression ratio, which affects human perception. 2.Enables accurate localisation in both the temporal and spatial frequency domains. 3. Cropping and scaling are vulnerable.	1. Computing costs may be higher. 2. There is a higher level of computational complexity. 3. It's possible that the compression time will be longer. 4. Image noise may emerge at the image's edges.
DFT	Rotation, scaling, and translation are all terms used in DFT (RST). As a result, it is utilised to correct geometric distortions.	1. Difficult implementations 2.The cost of computing could be higher.

LSB	1. Visual quality degradation is minimal. 2. Simple to use and comprehend. 3. Perceptual transparency is high.	1. Extremely sensitive to background noise. 2. Cropping and scaling assaults are possible. 3. Extremely vulnerable to attacks.
Correlation	Improves the watermark's robustness by boosting the gain factor.	Image quality may suffer as a result of the extremely high gain factor increase.

VI. APPLICATION OF WATERMARK METHODOLOGY

Because of the considerable thoroughness on applications, such as 1.Copyright protection, digital watermarking may also remain outdated.

2. Monitoring of the source (different recipients reach differently watermarked content).

3. Government broadcasting (television information oft contains watermarked video beside worldwide agencies).

4. Authentication via video

5. Software hobbling over screen mould or video modifying software programme programmes, in order to encourage customers to buy the ideal model in line with lift it.

6. Communitarian network content management.

7. Copying Control and Fingerprints.

8. Authenticity of Content.

9. Broadcasts Supervision.

VII. CONCLUSION

We looked at a variety of factors related to digital watermarking technologies and applications in this research. A rapid and comparative analysis of watermarking technologies can also be useful for current research in adjacent fields. We also divided the watermarking algorithms into categories based on their spatial and transform domains. Watermarking, which is associated with the statistical concealing field, has gotten a lot of attention recently in the lookup pastime. In its field, there is a tussock about work beginning to be carried out into one of kind branches. We align tactics based on exceptional domains where data is embedded. We've decided to limit the survey to only images.

REFERENCES

[1] Akhil Pratap Singh,Agya Mishra,"Wavelet based Watermarking on Digital Image",Indian Journal of Computer Science and Engineering,Vol.1,No.2,2011,pp86-91.

[2] Amit Kumar Singh, Nomit Sharma, Mayank Dave, Anand Mohan, ―A Novel Technique for Digital Image Watermarking in Spatial Domain‖, 2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing.

[3] From Wikipedia http://en.wikipedia.org/wiki/Digital_watermarking

[4] P.W. Chan and M. Lyu, "A DWT-based Digital Video Watermarking Scheme with Error Correcting Code," Proceedings Fifth International Conference on Information and Communications Security (ICICS2003), Lecture Notes in Computer Science, Springer, Vol. 2836, pp. 202-213, Huhehaote City, Inner-Mongolia, China, Oct. 10-13, 2003.

[5] Jiang Xuehua, ―Digital Watermarking and Its Application in Image Copyright Protection‖, 2010 International Conference on Intelligent Computation Technology and Automation.

[6] Lakshmi Priya C V and Nelwin Raj N R," Digital watermarking scheme for image authentication", International Conference on Communication and Signal Processing, April 6-8, 2017, India.

[7] Malika Narang,Sharda Vashisth,"Digital Watermarking using Discrete Wavelet Transform",International Journal of Computer Applications (0975-8887) Volume 74– No. 20,July 2013,pp34-38.

[8] Pereira, S., Pun, T., "Robust Template Matching for Affine Resistant Image Watermarks," in IEEE Transactions on Inage Processing, vol. 9, no. 6, pp. 1123-1129, June 2000.

[9] Ravi K Sheth,Dr. V V Nath,"Secured Digital Image Watermarking with Discrete Cosine Transform and Discrete Wavelet Transform method",IEEE International Conference on Advances in Computing,Communication,& Automation (ICACCA) (Spring),2016.

[10] Solachidis, V & Pitas, I 2001, 'Circularly Symmetric Watermark Embedding in 2-D DFT Domain', in IEEE Transactions on Itnage Processing, vol. 10, no. 11, pp. 1741-1753.

[11] Vidyasagar M. Potdar, Song Han, Elizabeth Chang," A Survey of Digital Image Watermarking Techniques", 3rd IEEE International Conference on Industrial Informatics Aug. 2005.

[12] Alok Kumar Chowdhury and Md. Ibrahim Khan, "A Tutorial for Audio Watermarking in the Cepstrum Domain", Smart Computing Review, vol. 3, no. 5, October 2013.

[13] Palak Patel and Yask Patel, " Secure and authentic DCT image steganography through DWT – SVD based Digital watermarking with RSA encryption" published in Communication Systems and Network Technologies (CSNT), 2015 Fifth International Conference on 4-6 April 2015.

.