

ADVANCED IMAGE WATERMARKING AND SECRET DATA HIDING FOR MOBILE COMMUNICATION BY USING ADAPTIVE NEURO FUZZY INFERENCE SYSTEM: A SURVEY

Mrs.Appisetty Venkata Lakshmi, CMR Institute of Technology Hyderabad

Abstract— - In the digital era, protection and illicit redistribution of digital media has proven to be a vital challenge. Watermarking software is among the most essential strategies for preserving copyrights and certifying ownership, as well as preventing software piracy. The evolution of communication technology has resulted in a vast number of digital data that must be safeguarded. Watermarking is a strategy for hiding confidential info in an original signal in a way that enhances the signal's overall performance. Multiple watermarking, because more numerous one watermark is inserted into a single multimedia product, is another topic that is attracting interest in the case of digital image watermarking. A trademark or copyright message is discreetly encoded in the medical image using only a digital watermarking method. ANFIS has been developed by many scholars to include a watermark in the primary (cover) image. The embedding locations during watermarking can be selected by regions of interest (ROIs). An optimized-quality component is offered to limit the differentiation of unique and watermarked unaccompanied values. Firstly, the height signal-to-noise ratio (PSNR) is described, which is a mould form performance index. Then, as per the quantization approach, an optimized-quality functional to that quantity connects the performance index.

The proposed approach generates excessive top signal in terms of noise ratio (PSNR) for watermarked photographs while also achieving excessive values for normalised contextual connection (NCC) for the recovered watermark.

Keywords—*Image Watermarking; Copyright material, cryptographic techniques, LWT, MSE, PSNR.*

I. INTRODUCTION

Privacy refers to an individual's or a collective's ability to keep information about themselves or their group private and only expose it selectively [1]. The link between data gathering and dissemination, technologies, public privacy rights, and legal difficulties is known as data privacy or data security [1]. Until enough systems get linked to the internet, it has now become increasingly crucial. Digital marketing and advertising, massaging, actual data delivery, data sharing, cooperation among computers, merchandise ordering, transactions, digital repositories and library resources, web magazines and newspapers, network audio and video, personal interaction, and many other applications have sprung up as a result of the development of high computer systems and the Online World. Due to advancements in technology, the cost efficiency of creating software in the type of electronic images and video sequencing via internet transmission has substantially increased.

This method is excellent since it achieves a theoretical benchmark of the embedding process through the use of watermark approaches. But at the other hand, spatial area watermarking has the capability of performing partial transformations directly on image pixels.

Digital watermarking is the way of introducing a watermark onto digital data. It's a method of incorporating inconspicuous logos, labels, data, or patterns into digital data [2]. Steganography is linked to the concept of digital watermarking. Digital watermarking is indeed a method of hiding a total secrecy or personal notification to provide copyright laws and data integrity. Encased writing is presented as a means of hiding a powerful message in an encased media, whereas digital watermarking is a method of hiding a hidden or personal notification to provide copyrights and data integrity. Watermarking digital images is a novel technology that can be used in medical, military, and archive applications. The embedded watermarks, which can be in the textual form, image, audio, or video, are hard to remove and usually undetectable. The insertion of a secret watermark in electronic

information, regardless of how inconspicuous it is. However, the resulting embedded digital data suffers some deterioration. Reversible watermarking, which would be regarded as the best technique over encryption, has been used to circumvent this and obtain the original data. In cryptography, the generated data may well not be visible or understood after encryption, and this could result in the loss of semantics in the host data, which wasn't the case with watermarking. Numerous watermarking techniques are used to embed multiple watermarks in digitized data in real - time. A digital watermark, also known as a digital signature, ensures the legitimacy of a document. A watermark might be unique towards each copy (for example, to indicate the intended destination) or shared by several copies (e.g. to identify the document source).

Watermarks are image alterations like this. The act of adding (embedding) a watermark signal to the host signal is known as watermarking. To make a statement about the object, the watermark can be recognised or retrieved afterwards. Figure 1 depicts a general system for digital watermarking. A logo image, a visually recognised binary image, or a binary bit stream could all be used as a watermark message. Some secret key is used at the embedder to embed a watermark into the host data. To produce the watermarked signal, the informational embedding procedure enforces minor signal modifications that are defined by the key and watermark. The key is known only by the data owner, and it is impossible to delete the message from either the data without knowing the key. The image is then transmitted through the transmission channel, which is watermarked.

There are two processes to extracting a watermark. One or more pre-processes are performed to the watermarked data during first phase to extract a vector named extracted watermark. The step two is to see if the extracted watermark is much like the original data by matching it to the standard watermark, which is the actual watermark. The second phase yields a confidence score that indicates how probable the original watermark is to be contained in the digital data.

A typical image watermarking system [5] is proposed in this study, which is essentially based on 3D Lifting wavelet seriously change (3D LDWT) and Singular Value Decomposition (SVD). In this approach, LDWT is applied to the image's ROI (region of interest) in compliance with the image's wavelet decomposition's particular frequency sub-bands. On the ROI's nasty frequency sub-band LL. From either the left individual cost matrix on all these elected blocks [3,] a pair of factors with similar characteristics is determined. The values for these pairs are changed by using a specific beginning in order to provide a sting to the watermark content. Appropriate starting point is established to achieve medical image and watermark object imperceptibility and resilience, respectively. One watermark picture (logo) and another text watermark have been utilised for authentication and identification of a distinctive scientific image. The watermark photo serves as authentication, while the textual content information serves as identification by representing an electronic patient record (EPR). At the recipient's end, an extract of both watermark facts is created using the same contrast intention as the embedding operation.

Several nonlinear classification issues have been solved using artificial intelligence, such as neural networks, fuzzy logic inferences, genetic algorithms, and expert systems [4-5]. The capacity to represent nonlinear input-output interactions using a set of qualitatively if-then rules is one of the key benefits of a Fuzzy Logic System (FLS). From the other hand, the essential benefit of an Artificial Neural Network (ANN) is its intrinsic learning capability, which allows the networks to enhance their performance over time. The precise learning and adaptive skills of neural networks, as well as the generalisation and quick learning capabilities of fuzzy logic systems, are the core properties of neurofuzzy networks. A neurofuzzy system is a hybrid of neural networks and fuzzy systems in which the neural network determines the fuzzy system's characteristics. The system parameters are automatically tuned using a neural network. The ANFIS is a very powerful method for modelling nonlinear and complicated systems with little input and output training data and high precision. The neuro fuzzy system, which combines the learning capabilities of a neural network with the benefits of a rule-based fuzzy system, can greatly increase performance and provide a method for incorporating observed data into the classification process. In a neural network, training is essentially what

constructs the system. The system is constructed using fuzzy logic concepts and then enhanced using neural network training methods in a neuro fuzzy approach.

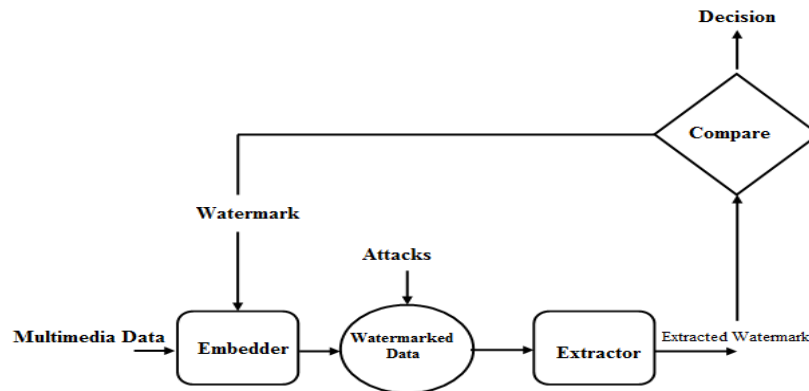


Figure 1: Watermarking System

II. LITERATURE SURVEY

Both the spatial and transform domains are used to represent and store images. In the transform domain, images are expressed by frequencies, while in the spatial domain, images are expressed by pixels. In layman's words, transform domain refers to the segmentation of an image into several frequency bands. Numerous reversible transformations, such as the Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), and Discrete Fourier Transform (DFT), can be used to convert an image to its frequency representation (DFT). Each of these transformations can have its own set of properties and depicts the image in a unique way. Adjusting these values, i.e. the transform domain coefficients, allows watermarks to be placed within images. Basic watermarks could be inserted in photos in the spatial domain by changing the pixel values or even the Least Significant Bit (LSB) values. By changing the transform domain parameters, more resilient watermarks could be inserted in the transform domain of images. Cox et al. published "Secure Spread Spectrum Watermarking for Multimedia" [6] in 1997, which is among the most cited papers (cited 2985 times as of April 2008 according to Google Scholar), and on which most subsequent research focused. Despite the fact that spatial domain analysis methods are unable to withstand most typical attacks like as compression, high pass or low pass filtering, and so on, researchers have developed spatial domain based schemes. To begin, brief descriptions of various well-known spatial domain-based methods are presented as follows [6]:

Tavassoli et al. (2010) [7] suggested approach to watermark digital image with cover image, consisting of two stages: first, embedding is recognised using an Adaptive Neuro-Fuzzy Inference System (ANFIS), then new changes are applied to these pixels using the Fuzzy Wavelet Shrinkage algorithm in the final stage (FWS). On several grayscale images, this strategy is tested. Use well-known approaches like the Median Filter (MF), Center Weighted Median Filter (CWMF), Signal Dependent Rank Order Mean Filter (SD-ROMF), Iterative Median Filter (IMF), Fuzzy Filter (FF), and Impulse Noise Detection and Estimate to compare this (INDINE).

Rhoads [8] described a way for modifying each pixel by adding or subtracting small random amounts. The LSB of every pixel is compared against a binary mask of bits to compute addition or subtraction. The random value is added if the LSB is equal to the matching mask bit, else it is subtracted. The watermark is removed by estimating difference amongst the original and watermarked images but then pixel-by-pixel inspecting the sign of the discrepancy to see if it matches the original additions and subtractions. Although this approach doesn't use the perceptual significance, it is suggested that the high frequency disturbance be prefiltered to give some lowpass filtering resilience. The issue of malicious packets is not addressed in this system.

The writers of [9] came up with analytical equations for possibilities P-, P+ of false null and false affirmative watermark identification. Its concept implies a cumulative watermark and an identification

step depending on a carrier signal. Clear watermarks and watermarks with low pass properties are both taken into account. Using a first order segmented periodicity function, the host picture is regarded as chaos. The signature to image average power is used to calculate the chances P^- and P^+ . The study finds that black lines with short pass properties have improved recognition failure rates.

This system is resistant to geometrical challenges. De Rosa et al. developed a method for inserting watermarks by directly changing the DFT amplitude function's mid frequency regions [10]. Ram Kumar et al. have introduced a DFT-based data concealing strategy in which the scale part of the DFT coefficients was changed. According to their calculations, magnitude DFT resists practical encoding, which could be related to the reality that majority practical compression techniques strive to optimise PSNR. As a result, employing magnitude DFT to discover the flaw in most feasible compression techniques is a viable option.

Watermark sensors depending on an extended Gaussian model, rather than the commonly used pure Gaussian assertion, can increase the efficiency of DCT-domain correlation-based watermarking systems [11]. The writers in [11] offered analytical expressions that can be used to represent the effectiveness estimated for a specific image and analyse the impact of image features and system factors (– for example watermark length) on its final performance through conducting a theoretical analysis for DCT-domain watermarking techniques for visuals. Moreover, the findings of this study could aid in identifying the appropriate detection threshold T for a specific false positive rate. The writers of [11] argued that removing the perfect Gaussian noise assumption could result in significant performance benefits.

Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), and Discrete Wavelet Transform are few of the changes used in these systems (DWT). The fundamental benefit of the Discrete Fourier Transform (DFT) is that its components do not change after interpretation. DFT is a complex transform that divides a visual into two blocks, one for magnitude and one for phases. The phasing matrix is more important for visual acuity. As a result, incorporating the watermark in the phases matrix strengthens its defences to attacks (inducing however more degradation in the quality of the image). This is indeed consistent with discourse analysis, which asserts that frequency modulation seems to be more noise-resistant than amplitude modulation. Watermarking techniques which use the DFT transformation have their own set of drawbacks [12]. The corresponding significant variables must stay symmetric in addition to have true values for the picture luminosity or colors following the reverse DFT transform (IDFT). This regularity demand splits the given area for knowledge embedding in half, halving the scheme's potential. Some other issue is the vulnerability of DFT values, particularly phase components, to compression techniques (e.g. JPEG, MPEG).

III. TYPES OF DIGITAL WATERMARKING

The preceding are the one-of-a-kind types of watermarking depending on various watermarks:

Visible watermark:

Concerning the concept of trademarks and such, a visible watermarks manufacturer has partially expanded services of concept on logos. “These watermarks are ancient solely regarding images. These logos are inlaid between the image yet it are transparent. These watermarks cannot stay eliminated by way of cropping the middle piece about the picture. Further, such watermarks are out of danger against certain as statistical analysis. The drawbacks of visible watermarks are downfallen the quality regarding image or detection with the aid of visual capability only”. As a result, achieving them with dedicated programmes or devices is no longer possible. This type of watermark is commonly found in software programme user interfaces, maps, and visuals.

Invisible watermark:

As the name implies, an invisible watermark is one that is not apparent in the content. Only authorised individuals or agencies are able to identify it.”“This type of watermarks is used most in author authentications. This invisible watermark helps in finding unauthorized printer”.

Robust Watermark:

It uses watermarks that aren't apparent to the naked eye. It has a high level of resistance to image processing and assaults. This has a broad range of uses in copyright security and ownership verification.

Fragile Watermark:

It is stolen within the material as an invisible watermark, as the odour suggests. It is only licenced men and women who are able to identify it. “This type of watermark is arguably as old as author authentications. This Perdue watermark aids in the detection of unlicensed printers.”

Image watermarks are embedded in this robust watermark. It is still facing assault after photo processing. This has a lot of implications for copyright security and ownership verification.

Semi Fragile Watermark:

This watermark has both robust and subtle watermark characteristics. This is sensitive to signal alteration in terms of compliance. In the majority of circumstances, it is used to offer data authentication.

IV. WATERMARKING TECHNIQUES

Watermarking approaches for deception keep twins' main groups broadly categorised:

- Spatial Domain Watermarking
- Frequency Domain Watermarking

Spatial Domain Watermarking

Watermarking techniques were first proposed in the spatial realm, where copyrighted information is communicated by modifying image pixels on a force image. The placement of the Least Significant Bit is one of the instances in that class [9]. This domain is concerned with improving the pixels in a few randomly selected groups of photographs. It immediately loads the raw photo pixel statistics. However, image processing procedures have shown that spatial area approaches are vulnerable to ignoble assaults [12]. Some of its algorithms include LSB and SSM Modulation.

Least Significant Bit (LSB)

Watermarks including its LSB of the pixels are embedded in the first work on digital photo watermarking techniques. Provided an image containing pixels, every pixel animal is expressed by an 8-bit sequence, and the watermarks are placed in the image's residual (i.e., least significant) bit regarding select pixels. This method is useful in compliance with put in force because it does not produce sufficient distortion in compliance with the image; nonetheless, it isn't completely resistant to attacks. For example, an attacker should unquestionably randomise entire LSBs, effectively erasing the obtained data.

SSM Modulation Based Technique

Spread spectrum strategies are those in which power generated at a number of different frequencies is ranged and then dispersed over time. This is implemented for a variety of reasons, including the establishment of tightly sealed communications, enhancing resistance to natural trespass and jamming, and preventing detection. SSM-based fully watermarking techniques engage records by linear integrating the legion image with a baby pseudo cacophony signal that is modulated by the incorporated watermark when used after the connection regarding image watermarking [13].

Frequency (Transform) Domain Watermarking

These approaches are similar in because after spatial area watermarking, the quantities of selected frequencies remain altered. Because higher frequencies are at risk of being lost due to cover and scaling, the watermark sign is used after lower frequencies, but higher frequencies are used adaptively after frequencies that include essential parts of the original image [14]. The watermark is placed in frequency coefficients on the legion picture in the Frequency region. Due to the embedding of the watermark into the changing frequency coefficients of the updated image, frequency domain watermarking is more Herculean than spatial area watermarking[15]. Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), and Discrete Wavelet Transform are some of the more often used frequency domain watermarking technologies (DWT).

Discrete Fourier Transform (DFT)

Permanency The Fourier Transform (FT) is a verb that changes the frequency component of a non-stop function. It is resistant to geometric attacks such as rotation, scaling, cropping, and removal [16]. The Discrete Fourier Transform is required to provide an equal dramatically change due to discrete costly characteristics (DFT). The furthermore functions to that amount are no longer current do lay stated in digital photo processing, so the necessary regarding earth and/or cosine improved through a weighting function. This weighing factor is based on the Fourier Transform coefficients over the signal. The Fourier Transform allows for the investigation and processing of signals in their frequency domain by inspecting and altering their coefficients [17].

Discrete Wavelet Transform (DWT)

The multi-resolution overview is created using the Discrete Wavelet Transformation (DWT) of an image. For decoding image data, a multi-resolution presentation provides a simple hierarchical structure. The little print on an image at various resolutions usually depicts unique physical features over the image. These essential spots correspond to the major buildings that provide the photograph's information at a medium degree of resolution. DWT [18] and IDWT are two fundamental steps in wavelet transformation (Inverse DWT). DWT divides a digital signal into high-frequency and low-frequency quadrants. The mean frequency quarter is broken up again into a handful of larger components relating to excessive or horrible frequencies, and this process is repeated until the sign is completely dissected. Watermarking often employs 1-5 degree over decompositions. With the help of IDWT, the original signal from either the decomposed snapshot may be reconstructed. As a result of decomposition, several types of wavelets exist. In most cases, DWT software divides an image into IV under leash (Figure 2), as well as distinct intents on vertical and horizontal coefficients. The manifest objectives across the images are represented by the LH, HL, or HH tributary chains, while the approximation on the image is represented by the LL subpart. As a result of the 2-level wavelet decomposition, the LL sub-band is further decomposed to obtain the next underhand level (Figure 2). The software determines the level of deconstruction performed. The current action takes into account breakdown after two stages [19].

3-LEVEL LIFTING WAVELET TRANSFORM

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 [20].

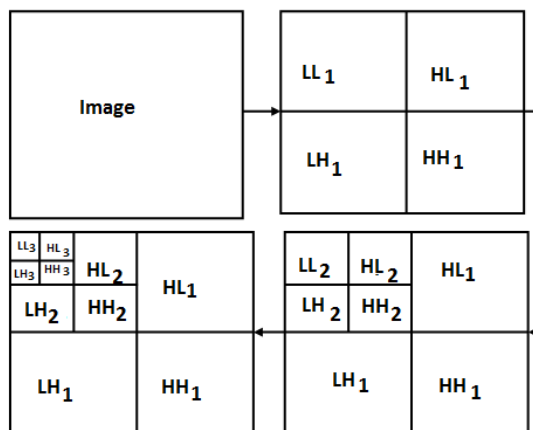


Figure 2: 3-Level LWT Decomposition

Discrete Cosine Transform (DCT):

A method for transforming a signal within frequency components is the variant cosine transform. It shows recordings in terms of frequency space as an alternative to a large space. In comparison to spacial domain techniques, DCT-based watermarking strategies are husky. Such algorithms are well-suited to simple image technology tasks such as obnoxious skip filtering, brightness, and contrast coordinating during blurring. It is difficult to implement in a consistent manner and is computationally costly. At the same time, they are minor in comparison to geometrical attacks such as rotation, scaling, cropping, and so on.

V. Adaptive Neuro Fuzzy Inference Systems (ANFIS)

The fuzzy logic with neural network techniques are combined in an ANFIS, which is a type of fuzzy inference system. ANFIS is a sort of artificial neural network centered on fuzzy logic inference systems of the Takagi-Sugeno type. The optimum value of design variables of the fuzzy inference system are determined using an artificial neural network. By employing data sets to train the artificial neural network, the fuzzy inference system has obtained an adaptive characteristic. A hybrid approach combining the widely known back-propagation active learning with the regression method is utilised to train the neural network [21].

The fuzzy logic system has a number of drawbacks;

- The requirement for identifying the rule base, which is normally accomplished by consulting an expert. This is really a time-consuming and problematic process.
- Evidently, the membership functions required for the construction of fuzzy sets must be determined. How would the coefficients of the Gaussian membership function be, for illustration, if Gaussian membership functions were selected??

ANFIS enables for the determination of the rule base and membership functions utilizing data sets for this objective.

The rules can be built but use a decompositional technique thanks to the ANFIS architecture. ANFIS is a multi-layer feed-forward network with two types of networks: adaptive and fixed. Every node (neuron) provides a particular function on the received signal. The rules are retrieved at the particular node level of such neural network, then aggregated to reflect the system's global dynamics (Jang 1993). The preliminary stated input-output pairings are generated by fuzzy if-then rules with suitable

membership functions, and so these membership functions acquire their final forms throughout training owing to regression and optimization techniques.

For a variety of parameters, the gradient vector involves measurement of how well the system is imitating the provided training data set. After obtaining the gradient vector, optimization methods are used to alter the parameters in order to lower a specified error criteria. Whenever the training as well as checking errors are still within an appropriate range, the system conforms.

The architecture and learning rules of adaptive networks have been described in the previous section. Except for piecewise differentiability, there are essentially no functional limitations on the node functions of an adaptive network. The only structural constraint on network setup is that it must be feedforward. The adaptive network's applications are immediate and vast in a variety of sectors due to these limited constraints. We present a type of adaptive networks that are functionally similar to fuzzy inference systems in this section. ANFIS is for Adaptive-Network-based Fuzzy Inference System, and it is the name given to the suggested design. We show how to decompose the parameter set so that the hybrid learning rule may be applied. We also show how to use the Stone-Weierstrass hypothesis with simplified fuzzy if-then rules to adapt the Stone-Weierstrass theorem to ANFIS and how well the radial basis function network relates to this type of simplified ANFIS.

The architecture of the ANFIS

For the sake of simplicity, we will suppose that the fuzzy inference system in question has two inputs and one output. Assume the rule base contains two Takagi and Sugeno-style fuzzy if-then rules [22]:

Rule 1: If x is A_1 and y is B_1 , then $f_1 = p_1x + q_1y + r_1$

Rule 2: If x is A_2 and y is B_2 , then $f_2 = p_2x + q_2y + r_2$

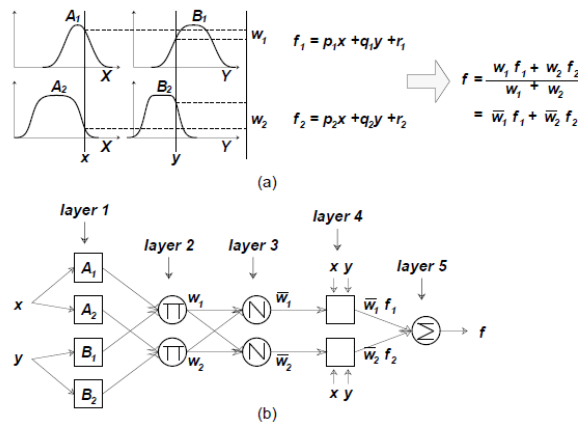


Figure 3: (a) Type-3 fuzzy reasoning; b) equivalent ANFIS (type-3 ANFIS).

then the type-3 fuzzy reasoning is illustrated in Figure 3(a), and the corresponding equivalent ANFIS architecture

(type-3 ANFIS) is shown in Figure 3(b).

V. APPLICATIONS OF DIGITAL IMAGE WATERMARKING

Inside of dense applications, digital idea watermarking is nothing new. The following are the details:

1. Broadcasts Supervision: Advertisers want to make sure they get all of the air time they pay for from broadcasters (Japan 1997 [23]). The use of human observation to monitor the broadcast and assess the uniqueness by seeing or hearing is a nontechnical method that is mistake prone and costly. As a result, an auto-identifying system should be in place, capable of storing the broadcast's unique identifiers. There are numerous approaches for storing the identifying code in the file header, such as cryptography, however the data is unlikely to survive any type of modification, including a format change. Watermarking is an obvious choice for information surveillance. The Watermark is embedded in the content and is compliant with the broadcast apparatus currently in use. Although, as contrasted to cryptography, where the code is stored in the file header, embedding the identification code is

extremely difficult. It also has an impact on the work's visual quality. Nonetheless, several companies use watermarking to safeguard their broadcasts.

2. Ownership Affirmation: To verify his ownership, a lawful owner can retrieve the watermark from digital content. Textual copyright notices have limits because they can easily be removed. Copyright notices put on physical documents are not compatible with digital information. Although, in order to make them unobtrusive, text copyright might be placed in an irrelevant part of the document [24]. In comparison to a text mark, a watermark that is undetectable and inseparable is the greatest solution for ownership identification. The watermark was being used not only to identify who owns the copyright to the content, but also to prove who owns the document. Ability to extract the hidden information from either the watermarked document can be used to determine ownership.

3. Transactions Tracing: Transaction tracing is sometimes known as fingerprinting, because each copy of the work is individually recognised, much like a person's fingerprint. The beneficiary of each legitimate dissemination of the work could be recorded in the watermark. Each copy has a separate watermark embedded by the owner. Will the owner be able to track down the traitor if the work is misappropriated? For transaction tracking, visible watermarking is used, although invisible watermarking is far superior. In the film industry, for example, daily videos (also known as dailies) are given to those involved with the project. Because the studios use visible text on the edge of the screen to identify the copy of dailies when the videos are released to the press, the studios utilize visible text on the edge of the screen to identify the copy of dailies. As a result, the watermark is preferable because the text can be readily deleted.

4. Authenticity of Content: The act of establishing or validating whether an image is real or not by confirming the consistency of watermarked data and ensuring that the data has not been tampered with. The phrase authentication has a wide range of interpretations. Can a person, for example, view or receive an authority that determines if a piece of art is authentic or not? Finally, whether or not the content of an object remains intact after transmission via the internet is a decision. Many cultural institutions devote time and resources to developing new technologies for picture documentation and the creation of digital libraries, among other things. At the same time, because they have both ownership and expert judgments, these organisations can ensure the authenticity of the works of art they own. Numerous issues arise when these pieces of art are digitised and distributed on the internet. Several digital photographs obtained on the internet usually have various changes while ostensibly representing the same work of art. Trustworthy cameras, surveillance footage and remote sensor applications, digitized insurance payout evidence, journalistic imagery, and digital asset management systems are all using watermarking for authentication. Commercial uses, such as GeoVision's GV-Series video on demand for digital video surveillance to avoid tampering, are projected to develop as digital content industries do. Using system resources, the digital product can simply be modified with. Watermarking is a tamper-detection method in which the authenticating mark (watermark) cannot remain with the work after even minor changes. The system, on the other hand, does not care if the work is compressed or if significant modifications are required. This results in semi-fragile watermarking, in which the system survives favourable manipulations but is vulnerable to significant manipulations [5].

5. Copying Control and Fingerprints: Copying control and biometric identification are used to prevent unlawful copies of content from being made. This problem is very comparable to the content transactions tracking. A watermark can be embedded in digital files that identifying the copy's buyer (i.e. serial number). If later unauthorised copies are discovered, the owner will be able to track down the source of the illicit copies.

VI. BENEFITS OF DIGITAL WATERMARKING

- Simple to use and comprehend. Image quality is not degraded significantly. Perceptual transparency is high.
- The gain multiplier can be increased, increasing robustness. High level of resistance to a wide range of attacks.

- This approach conceals data within an image's random texture information.
- Because the watermark is incorporated in the middle frequency components, the image's visibility is unaffected, and the watermark is unaffected by any attack.
- Enables accurate localisation in both the temporal and spatial frequency domains. The compressing ratio is increased, which is important for human perceptions.
- DFT is RST invariant (rotating, scaling, and translating). As a result, it can be used to correct misalignments.

VII. PROBLEMS WITH DIGITAL WATERMARKING

- It is lacking in basic sturdiness. Noise is a threat. Cropping and scaling are both possible.
- Due to the extremely high gain factor, image quality suffers.
- It can only conceal a very little amount of data.
- This approach is only useful in places where there are a lot of arbitrary texture pictures.
- Block wise DCT undermines the system's invariance features. During the quantization process, certain high frequencies components are often suppressed.
- Computing costs may be greater. Compression time is extended. Near the borders of photos or video frames, there is noise or blur.
- The implementation is difficult. Computing costs could be greater.

VIII. CONCLUSION

Various types of watermarking approaches were investigated in this same article. The geographical or frequency area wherein the watermark is inserted has been used to characterize watermarking methods. In terms of processing, frequency approaches outnumber spatial techniques. We offered a watermarking summary and briefly reviewed various watermarking approaches in this study. A short and comparative review of watermarking approaches is also offered, along with their benefits and drawbacks, which can aid in emerging areas of research. An ANFIS based image watermarking system has been developed in this paper. This technique uses an alpha mixing method to incorporate the cover images watermark, which may be recovered by extraction. The survey results reveal that because the watermarked image's virtue is only determined by the scaling component, the recovered watermark is unaffected by the scalability factor. The health of some images and the watermark is higher for 3 degree distinct wavelet transform after 1 & 2 stage variant wavelet transform, according to a survey. It also means that the healthy cover image or watermark image is on par with the unique images in terms of conformance.

REFERENCES

- [1] Macq. B.M. & Quisquater. J.J. (1994), "digital Image multiresolution encryption", The journal of the Intraactive Multimedia Association Intellectual property project. L (1) 179-206
- [2] From Wikipedia http://en.wikipedia.org/wiki/Digital_watermarking
- [3] 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.
- [4] Jang J-SR. ANFIS adaptive-network-based fuzzy inference system. IEEE Trans Syst Man Cyber 1993;23(3):665–85..
- [5] CHAPTER 2: LITERATURE REVIEW, Source: Internet
- [6] I. Cox, J. Kilian, T. Leighton, and T. Shamon, "Secure spread spectrum watermarking for multimedia," IEEE Transactions on Image Processing, vol. 6, no. 12, pp. 1673–1687, 1997.
- [7] S. Tavassoli, A. Rezvanian and M. M Ebadzadeh, "A New Method for Impulse Noise Reduction from Digital Images Based on Adaptive Neuro-Fuzzy System and Fuzzy Wavelet Shrinkage,"

- Proceedings of International Conference on Computer Engineering and Technology (ICCET'10), Vol. 4, pp. 297-301, 2010.
- [8] Rhoads G.B., "Indentification/authentication coding method and apparatus", World Intellectual Property Organization, vol. IPO WO 95/14289, 1995.
- [9] Muftic, S. (2010). Privacy Issues and Solutions in Real and in Digital Worlds. Presentation at the AAAS 2010 Conference – San Diego, February 20, 2010. In 'http://ec.europa.eu/dgs/jrc/downloads/jrc_aaas2010_privacy_muftic.pdf'.
- [10] T. Komatsu, T. Igarashi, K. Aizawa, and T. Saito, "Very high resolution imaging scheme with multiple different-aperture cameras," *Sinal Processing: Image Commun.*, vol. 5, pp. 511-526, Dec. 1993.
- [11] Hernández J.R., Amado M., Gonzalez F.P., " DCT-Domain watermarking techniques for still images: Detector performance analysis and a new structure", *IEEE Transactions of Image Processing*, vol. 9, pp. 55-68, Jan. 2000.
- [12] Satendra kumar, Ashwini Kumar Saini, Papendra Kumar, "SVD based Robust Digital Image Watermarking using Discrete Wavelet Transform", *International Journal of Computer Applications*, Volume 45– No.10, May 2012.
- [13] Vandana Tehlani, "A New Fragile Approach for Optimization in Invisible Image Watermarking by Using Symmetric Key Algorithms", *International Journal of Advanced Research in Computer Engineering & Technology*, Volume 1, Issue 5, July 2012.
- [14] Gurpreet Kaur, Kamaljeet Kaur, "Image Watermarking Using LSB (Least Significant Bit)", *International Journal of Advanced Research in Computer Science and Software Engineering*, Volume 3, Issue 4, April 2013.
- [15] Kusuma Kumari B. M, "A Survey of Digital Watermarking Techniques and its Applications", *International Journal of Science and Research (IJSR)*, Volume 2, Issue 12, December **2013**.
- [16] Pravin M. Pithiya, "DCT Based Digital Image Watermarking, De-watermarking Authentication", *International Journal of Latest Trends in Engineering and Technology (IJLTET)* ISSN: 2278-621X ,Vol. 2 Issue 3 May 2013.
- [17] Senthil Nathan.M, Pandiarajan.K, Baegan.U, "Digital Image Watermarking Basics", *IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)*, Volume 8, Issue 1, Sep. - Oct. **2013**.
- [18] Pratibha Sharma, Shanti Swami, "Digital Image Watermarking Using 3-level Discrete Wavelet Transform", *Conference on Advances in Communication and Control Systems 2013 (CAC2S 2013)*, pp129-133.
- [19] Jalpa M.Patel, Prayag Patel, "A Brief Survey on Digital Image Watermarking Techniques", *International Journal For Technological Research In Engineering* Volume 1, Issue 7, March 2014.
- [20] 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.
- [21] D. A. Wismer and R. Chattergy. *Introduction to nonlinear optimization: a problem solving approach*, chapter 6, pages 139–162. North-Holland Publishing Company, 1978.
- [22] T. Takagi and M. Sugeno. Derivation of fuzzy control rules from human operator's control actions. *Proc. of the IFAC Symp. on Fuzzy Information, Knowledge Representation and Decision Analysis*, pages 55–60, July 1983.
- [23] CHAPTER 2: LITERATURE REVIEW, Source: Internet <http://ippr-practical.blogspot.in>
- [24] D. Mistry, " Comparison of Digital Watermarking Methods" (*IJCSE*) *International Journal on Computer Science and Engineering*, vol. 02, no. 09, (2010), pp. 2805-2909.