



IJRASET

International Journal For Research in
Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 4 Issue: VI Month of publication: June 2016

DOI:

www.ijraset.com

Call:  08813907089

E-mail ID: ijraset@gmail.com

A Survey on Digital Watermarking with Wavelet Transform Domain

Pankaj Pandey¹, Sunil Sharma²

¹M.Tech Scholar Dr. C. V. Raman University, Kargi Road Kota Bilaspur,

²Asst Professor Dr. C. V. Raman University, Kargi Road Kota Bilaspur

Abstract— Digital video watermarking is a method for embedding some data into digital video sequences e.g. text, audio, image, video. Digital watermarking was developed to provide the copy right protection and owners' authentication. In this survey paper, we survey on video watermarking approach using 2 Level- Watermarking Technique and secure from removal attacks. We compatible with many attacks and remove from it.

Keywords— Video Watermarking, Watermarking Attacks, Wavelet Transform, DWT.

I. INTRODUCTION

Today Digital Watermarking is a rapidly developing area with various raising applications in computer science and engineering. Digital media is available in huge scale now a day and can be very easily copied and spread rapidly. It is very easily available to people to get the copy of those digital media. Consequently a large number of unauthorized copies are spread out over market, effect of which is the loss in publishing industries. The content owner has to use some protection mechanism like encryption or digital watermarking. Encryption is no longer adequate for copy right protection and authentication, which is why digital watermarking is being used widely. Watermarking is a method of embedding information in invisible and robust manner. Copy and tempering of video is quite easy today so, in order to protecting copy right, digital video watermarking technology taken as an important and more urgent component. Recently, video based applications such that video conferencing, videophone, set-top box, video broadcasting, video-on-demand, wireless videos, and internet multimedia are becoming more and more popular and has increased the demand for a secure distribution of videos. This technique is used in almost all kinds of tasks like human computer interface. We know an internet is the fastest medium of transferring data to any place in a world. As this technology grown up the threat of piracy and copyright very obvious thought is in owners mind. So Watermarking is a process of secure data from these threats, in which owner identification (watermark) is merged with the digital media at the sender end and at the receiver end this owner identification is used to recognize the authentication of data. This technique can be applied to all digital media types such as image, audio, video and documents. From many years researchers and developers worked in this area to gain best results. The watermark contains information about the origin, ownership, destination, copy control, transaction etc. Potential applications of digital watermarking include tracking, copy control, authentication, legacy system transaction enhancement and database linking etc. An important characteristic of digital watermarking is robustness and imperceptibility against various types of attacks or common image manipulation like rotation, filtering, scaling, cropping and compression. The efficiency of digital watermarking algorithms is totally based on the robustness of the embedded watermark against various types of attacks.

II. DIGITAL WATERMARKING

Digital watermarking is nothing but a digital code embedded into digital cover content e.g. text, image, audio and in our case video sequence. A watermark can be any random or serial number, ownership identifier, information about the creator, date etc. It can carry any unlimited information, but as more information watermark carry, the original information will be more vulnerable. So the amount of watermark must be limited by the size of an original message, here video sequence. As watermark prefers to robustness, it carries tens to thousands bits per one video frame.

Digital Video: Digital video is a sequence or collection of consecutive still images.

Payload: The amount of information that can be embedded into the video sequence.

Security: In watermarking the security is assured in the same way as in encryption. Though the algorithm of watermarking process is public, security depends on the choice of the key

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

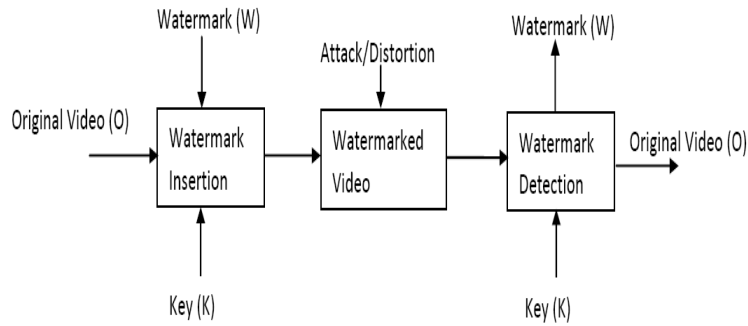


Fig 1. Video Watermarking Terminology

A. Properties of Video Watermarking

For digital video watermark some most important characteristics or properties of watermarking process are required. Such as, Robustness—The watermark should be impossible to remove from watermarked video, without the sufficient knowledge of an embedding process. The robust one is specially designed to withstand a wide range of attacks.

- 1) *Imperceptibility*: The watermark embedded into the digital video sequence should be invisible to Human Vision System (HVS).
- 2) *Unambiguous*: The extracted watermark should uniquely identify the original owner of the video.
- 3) *Loyalty*: A watermark has a high reliability, if the degradation it causes is very difficult to perceive for the viewer.
- 4) *Computational Cost*: Digital video watermark system includes, embedding and detecting process both should be fairly fast and should have low computational complexity.
- 5) *Interoperability*: Watermark system must be interoperable for the compressed and decompressed operations.
- 6) *CBR (Constant Bit Rate)*: In the bit stream domain, watermarking should not increase the bit rate.
- 7) *Random detection*: In video watermarking the detection of watermark can be done in any position of video.
- 8) *Blind detection scheme*: Non-blind detection scheme require the original data, but for video sequence it is very inconvenient to use original data because of its huge content compare to image. While a blind detection scheme doesn't require an original data, so it is useful for video watermarking.

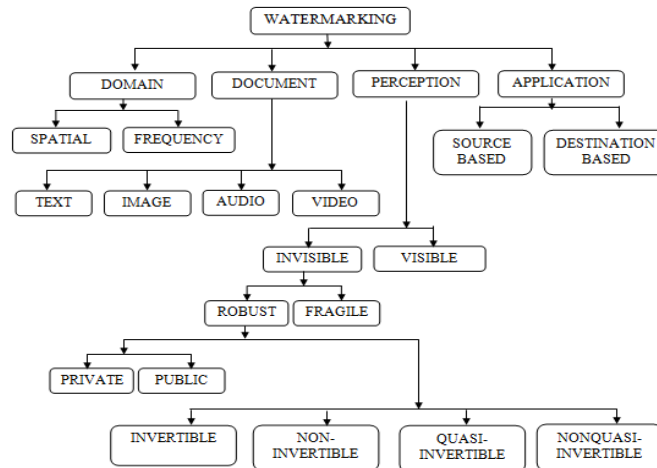


Fig 2: Types of watermarking

III. WATERMARKING TECHNIQUES

Watermarking is the method to hide the secret information into the digital media using some strong and appropriate algorithm. Algorithm plays a vital role in watermarking as, if the used watermarking technique is efficient and strong then the watermark being embedded using that technique cannot be easily detected. The attacker can only destroy or detect the secret information if he know the algorithm otherwise it is critical to know the watermark. There are various algorithms present in the today scenario that are used to hide the information. Those algorithms come into two domains, Spatial and Frequency domain.

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

A. Spatial domain

Spatial domain digital watermarking algorithms directly load the raw data into the original image [3]. Spatial watermarking can also be applied using color separation. In this way, the watermark appears in only one of the color bands. This renders the watermark visibly subtle such that it is difficult to detect under regular viewing. Spatial domain is manipulating or changing an image representing an object in space to enhance the image for a given application. Techniques are based on direct manipulation of pixels in an image. Some of its main algorithms are as discussed below:

- 1) *Additive Watermarking*: The most straightforward method for embedding the watermark in spatial domain is to add pseudo random noise pattern to the intensity of image pixels. The noise signal is usually integers like (-1, 0, 1) or sometimes floating point numbers. To ensure that the watermark can be detected, the noise is generated by a key, such that the correlation between the numbers of different keys will be very low.

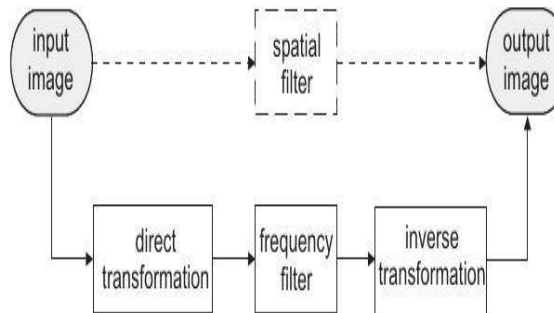


Fig: Brief Idea of Spatial and Frequency Domain

- 2) *Least Significant Bit*: Old popular technique embeds the watermark in the LSB of pixels. This method is easy to implement and does not generate serious distortion to the image; however, it is not very robust against attacks. The embedding of the watermark is performed choosing a subset of image pixels and substituting the least significant bit of each of the chosen pixels with watermark bits. The watermark may be spread throughout the image or may be in the select locations of the image. But these primitive techniques are vulnerable to attacks and the watermark can be easily destroyed. Such an approach is very sensitive to noise and common signal processing and cannot be used in practical applications.
- 3) *SSM Modulation Based Technique*: Spread-spectrum techniques are methods in which energy generated at one or more discrete frequencies is deliberately spread or distributed in time. SSM based watermarking algorithms embed information by linearly combining the host image with a small pseudo noise signal that is modulated by the embedded watermark.
- 4) *Texture mapping coding Technique*: This method is useful in only those images which have some texture part in it. This method hides the watermark in the texture part of the image. This algorithm is only suitable for those areas with large number of arbitrary texture images (disadvantage) [3], and cannot be done automatically. This method hides data within the continuous random texture patterns of a picture.
- 5) *Patchwork Algorithm*: Patchwork is a data hiding technique developed by Bender et alii and published on IBM Systems Journal, 1996[11]. It is based on a pseudorandom, statistical model. Patchwork imperceptibly inserts a watermark with a particular statistic using a Gaussian distribution. A pseudo randomly selection of two patches is carried out where the first one is A and the second is B. Patch A image data is brightened where as that of patch B is darkened (for purposes of this illustration this is magnified). The following are the steps involved in the Patchwork algorithm:

Generate a pseudo-random bit stream to select pairs of pixels from the cover data.

For each pair, let d be the difference between the two pixels.

Encode a bit of information into the pair. Let $d < 0$ represent 0 and $d > 0$ represent 1. Given that the pixels are not ordered correctly, swap them.

In the event that d is greater than a predefined threshold or if is equal to 0, ignore the pair and proceed to the next pair. Patchwork being statistical methods uses redundant pattern encoding to insert message within an image.

- 6) *Correlation-Based Technique*: In this technique, a pseudorandom noise (PN) pattern says $W(x, y)$ is added to cover image

$$I_w(x, y) = I(x, y) + k * W(x, y)$$

Where K represent the gain factor, I_w represent watermarked image ant position x, y and I represent cover image. Here, if we

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

increase the gain factor then although it increases the robustness of watermark but the quality of the watermarked image will decrease.

7) *Frequency domain*: Compared to spatial-domain methods, frequency-domain methods are more widely applied. The aim is to embed the watermarks in the spectral coefficients of the image. The most commonly used transforms are the Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT), the reason for watermarking in the frequency domain is that the characteristics of the human visual system (HVS) are better captured by the spectral coefficients [13]. Some of its main algorithms are discussed below:

B. Discrete cosine transforms (DCT)

DCT like a Fourier Transform, it represents data in terms of frequency space rather than an amplitude space. This is useful because that corresponds more to the way humans perceive light, so that the part that are not perceived can be identified and thrown away. DCT based watermarking techniques are robust compared to spatial domain techniques. Such algorithms are robust against simple image processing operations like low pass filtering, brightness and contrast adjustment, blurring etc. However, they are difficult to implement and are computationally more expensive. At the same time they are weak against geometric attacks like rotation, scaling, cropping etc. DCT domain watermarking can be classified into Global DCT watermarking and Block based DCT watermarking. Embedding in the perceptually significant portion of the image has its own advantages because most compression schemes remove the perceptually insignificant portion of the image. Steps in DCT Block Based Watermarking Algorithm

- (1) Segment the image into non-overlapping blocks of 8x8.
- (2) Apply forward DCT to each of these blocks
- (3) Apply some block selection criteria (e.g. HVS)
- (4) Apply coefficient selection criteria (e.g. highest)
- (5) Embed watermark by modifying the selected coefficients.
- (6) Apply inverse DCT transform on each block

C. Discrete wavelet transforms (DWT)

Wavelet Transform is a modern technique frequently used in digital image processing, compression, watermarking etc. The transforms are based on small waves, called wavelet, of varying frequency and limited duration. The wavelet transform decomposes the image into three spatial directions, i.e. horizontal, vertical and diagonal. Hence wavelets reflect the anisotropic properties of HVS more precisely. Magnitude of DWT coefficients is larger in the lowest bands (LL) at each level of decomposition and is smaller for other bands (HH, LH, and HL). The Discrete Wavelet Transform (DWT) is currently used in a wide variety of signal processing applications, such as in audio and video compression, removal of noise in audio, and the simulation of wireless antenna distribution. Wavelets have their energy concentrated in time and are well suited for the analysis of transient, time-varying signals. Since most of the real life signals encountered are time varying in nature, the Wavelet Transform suits many applications very well. One of the main challenges of the watermarking problem is to achieve a better tradeoff between robustness and perceptivity. Robustness can be achieved by increasing the strength of the embedded watermark, but the visible distortion would be increased as well. However, DWT is much preferred because it provides both a simultaneous spatial localization and a frequency spread of the watermark within the host image. The basic idea of discrete wavelet transform in image process is to multi-differentiated decompose the image into sub-image of different spatial domain and independent frequencies .

- 1) *Advantages of DWT over DCT*: Wavelet transform understands the HVS more closely than the DCT. Wavelet coded image is a multi-resolution description of image. Hence an image can be shown at different levels of resolution and can be sequentially processed from low resolution to high resolution.
- 2) *Disadvantages of DWT over DCT*: Computational complexity of DWT is more compared to DCT'. As Feig (1990) pointed out it only takes 54 multiplications to compute DCT for a block of 8x8, unlike wavelet calculation depends upon the length of the filter used, which is at least 1 multiplication per coefficient.

D. Discrete Fourier transforms (DFT)

Transforms a continuous function into its frequency components. It has robustness against geometric attacks like rotation, scaling, cropping, translation etc. DFT shows translation invariance. Spatial shifts in the image affects the phase representation of the image but not the magnitude representation, or circular shifts in the spatial domain don't affect the magnitude of the Fourier transform.

- 1) *Advantages of DFT over DWT and DCT*: DFT is rotation, scaling and translation (RST) invariant. Hence it can be used to recover from geometric distortions, whereas the spatial domain, DCT and the DWT are not RST invariant and hence it is

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

difficult to overcome from geometric distortions.

IV. DIGITAL WATERMARKING APPLICATIONS

A. Copyright protection

Digital watermarking can be used to identify and protect copyright ownership. Digital content can be embedded with watermarks depicting metadata identifying the copyright owners.

B. Copy protection

Digital content can be watermarked to indicate that the digital content cannot be illegally replicated. Devices capable of replication can then detect such watermarks and prevent unauthorized replication of the content.

C. Digital right management

Digital right management (DRM) can be defined as —the description, identification, trading, protecting, monitoring, and tracking of all forms of usages over tangible and intangible assets. It concerns the management of digital rights and the enforcement of rights digitally.

D. Tamper proofing

Digital watermarks which are fragile in nature, can be used for tamper proofing. Digital content can be embedded with fragile watermarks that get destroyed whenever any sort of modification is made to the content. Such watermarks can be used to authenticate the content.

E. Broadcast monitoring

Over the last few years, the number of television and radio channels delivering content has notably expanded. And the amount of content flowing through these media vehicles continues to grow exponentially. In this highly fragmented and fast changing market, knowing the real broadcast reality has become critical for content owners, copyright holders, distributors and broadcasters.

F. Fingerprinting

Fingerprints are the characteristics of an object that tend to distinguish it from other small objects. As in the applications of copyright protection, the watermark for finger printing is used to trace authorized users who violate the license agreement and distribute the copyrighted material illegally. Thus, the information embedded in the content is usually about the customer such as customer's identification number.

G. Access control

Different payment entitles the users to have different privilege (play/copy control) on the object. It is desirable in some systems to have a copy and usage control mechanism to prevent illegal copy of the content or limit the number of times of copying. A robust watermark can be used for such purpose.

H. Medical application

Names of the patients can be printed on the X-ray reports and MRI scans using techniques of visible watermarking. The medical reports play a very important role in the treatment offered to the patient. If there is a mix up in the reports of two patients this could lead to a disaster.

I. Image and content authentication

In an image authentication application the intent is to detect modifications to the data. The characteristics of the image, such as its edges, are embedded and compared with the current images for differences. A solution to this problem could be borrowed from cryptography, where digital signature has been studied as a message authentication method. One example of digital signature technology being used for image authentication is the trustworthy digital camera

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

J. Annotation and privacy control

Multi-bit watermarking can be used to annotate an image. For example, patient records and imaging details related to a medical image can be carefully inserted into the image. This would not only reduce storage space but also provides a tight link between the image and its details. Patient privacy is simply controlled by not keeping the sensitive information as clear text in human readable form, and the watermark can be further secured by encryption. Other usages of annotation watermarking are electronic document indexing and automated information retrieval.

K. Media forensics

Forensic watermark applications enhance a content owner's ability to detect and respond to misuse of its assets. Forensic watermarking is used not only to gather evidence for criminal proceedings, but also to enforce contractual usage agreements between a content owner and the people or companies with which it shares its content.

L. Communication enhancement

Today's smart phones are becoming the handheld computing device we carry with us 24/7 — no longer are they merely for talking or texting. More and more we look to our mobile phones to provide us with assistance, instant information, and to entertain us.

M. Content protection for audio and video content

Modern digital formats employed for sale or rental of commercial audio and video content to consumers—such as DVD, Blu-Ray Disc, and iTunes—incorporate content protection technologies that control access to and use of the content and limit its unauthorized copying and redistribution. Parties seeking to engage in unauthorized distribution and copying of protected commercial music or video content must circumvent the content protection to obtain a decrypted copy of the content.

N. Content filtering

The lean-back experience of watching television has radically changed over the last few years. Today people want to watch content in their own time and place. The proliferation of set top boxes (STB) in homes evidences this, as people want to watch video on demand or on a time-shifted schedule. Today, more than a device to watch films/series, sports or even play games, the STB has become an interactive device providing multiple services.

O. Communication of ownership and objects

Digital content continues to proliferate as today's consumers seek information and entertainment on their computers, mobile phones and other digital devices. In our cyber culture, digital has become a primary means of communication and expression. The combination of access and new tools enables digital content to travel faster and further than ever before as it is uploaded, dispersed, viewed, downloaded, modified and repurposed at breathtaking speed. Whether you are a global media corporation or a freelance photographer, the ability to communicate your copyright ownership and usage rights is essential.

P. Document and Image security

Consider documents and images that are generated in support of a major product launch. Corporate communications professionals face significant challenges in managing these assets through very complex sales and marketing channels. Images and documents are distributed to remote offices, agencies, distributors, dealers and more, and must be managed to ensure confidential information is not leaked before the launch date.

Q. Locating content online

The volume of content being uploaded to the web continues to grow as we rely more and more on the Internet for information sharing, customer engagement, research and communication. It has also become a primary sales tool and selling environment, providing an opportunity to showcase our products or services and attract buyers from around the world.

R. Audience measurement

In this new media world of insatiable content consumption, audience measurement is becoming more and more critical. Beyond the hard numbers of how many people are accessing a program, understanding who is watching, how they engage with the content,

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

when, where and through which media is essential for content providers, advertisers and broadcasters to better tailor their offerings and maximize impact.

S. Improved auditing

Media content of all types - television, music, movies, etc. - continues to proliferate and make its way onto many new consumer devices as well as many sites across the internet. Digital watermarking applications for auditing give all members within the value chain the ability to verify usage to support highly accurate billing and contract

V. WATERMARKING ATTACKS

There are various possible malicious intentional or unintentional attacks that a watermarked object is likely to subject to. The availability of wide range of image processing soft wares made it possible to perform attacks on the robustness of the watermarking systems. The aim of these attacks is prevent the watermark from performing its intended purpose. A brief introduction to various types of watermarking attacks is as under,

Removal Attack: Removal attacks intend to remove the watermark data from the watermarked object. Such attacks exploit the fact that the watermark is usually an additive noise signal present in the host signal.

Interference attack: Interference attacks are those which add additional noise to the watermarked object. Lossy compression, quantization, collusion, demolishing, remodulation, averaging, and noise storm are some examples of this category of attacks.

Geometric attack: All manipulations that affect the geometry of the image such as flipping, rotation, cropping, etc. should be detectable. A cropping attack from the right-hand side and the bottom of the image is an example of this attack.

Low pass filtering attack: A low pass filtering is done over the watermarked image and it results in a difference map composed of noise.

Forgery attack: The forgery attacks that result in object insertion and deletion, scene background changes are all tantamount to substitution.

Security Attack: In particular, if the watermarking algorithm is known, an attacker can further try to perform modifications to render the watermark invalid or to estimate and modify the watermark. In this case, we talk about an attack on security. The watermarking algorithm is considered secure if the embedded information cannot be destroyed, detected or forged.

Protocol Attack: The protocol attacks do neither aim at destroying the embedded information nor at disabling the detection of the embedded information (deactivation of the watermark). Rather than that, they take advantage of semantic deficits of the watermark's implementation. Consequently, a robust watermark must not be invertible or to be copied. A copy attack, for example, would aim at copying a watermark from one media into another without knowledge of the secret key.

Cryptographic attacks: Cryptographic attacks deal with the cracking of the security. For example, finding the secret watermarking key using exhaustive brute force method is a cryptographic attack. Another example of this type of attack is the oracle attack [7]. In the oracle attack, a non-watermarked object is created when a public watermark detector device is available. These attacks are similar to the attacks used in cryptography.

Active Attacks: Here, the hacker tries deliberately to remove the watermark or simply make it undetectable. This is a big issue in copyright protection, fingerprinting or copy control for example.

Passive Attacks: In this case, the attacker is not trying to remove the watermark but simply attempting to determine if a given mark is present or not. Cox et al (2002) suggest that, protection against passive attacks is of the utmost importance in covert communications where the simple knowledge of the presence of watermark is often more than one want to grant.

Collusion Attacks: In collusive attacks, the goal of the hacker is the same as for the active attacks but the method is slightly different. In order to remove the watermark, the hacker uses several copies of the same data, containing each different watermark, to construct a new copy without any watermark. This is a problem in fingerprinting applications (*e.g.* in the film industry) but is not the widely spread because the attacker must have access to multiple copies of the same data and that the number needed can be pretty important.

Image Degradation: These type of attacks damage robust watermarks by removing parts of the image. The parts that are replaced may carry watermark information. Examples of these operations are partial cropping, row removal and column removal. Insertion of Gaussian noise also comes under this category, in which the image is degraded by adding noise controlled by its mean and its variance.

Image Enhancement: These attacks are convolution operations that desynchronize the watermark information in an image. These

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

attacks include histogram equalization, sharpening, smoothing, median filtering and contrast enhancement.

Image Compression: In order to reduce the storage space and cut the cost of bandwidth required for transmitting images, images are generally compressed with JPEG and JPEG2000 compression techniques. These lossy compression methods are more harmful as compared to lossless compression methods. Lossless compression methods can recover the watermark information with inverse operation. However lossy compression techniques produce irreversible changes to the images. Therefore probability of recovering watermarked information is always very low.

Image Transformations: These types of attacks are also called synchronization attacks or geometrical attacks. The famous software Stir Mark uses small local geometrical distortions to invalidate watermark detection. Geometrical attacks include rotation, scaling and translation also called RST attacks. Some researchers focus on RST robustness while designing the robust watermarking systems, because it is fundamental problem. Besides RST transforms, image transformations also include other transforms such as aspect ratio change, shearing, reaction and projection

VI. CONCLUSION

In this paper we have presented digital watermarking faces like overview, framework, techniques, applications, challenges. In this paper we tried to give the complete information about the digital watermarking. Through digital watermarking we can provide the copy right protection and owner's authentication.

REFERENCES

- [1] R.G. Schyndel, A. Tirkel, and C.F Osborne, —A Digital Watermark, Proceedings of IEEE International conference on Image Processing, ICIP-1994, pp. 86-90, 1994.
- [2] Christine I. Podilchuk, Edward J. Delp, —Digital watermarking: Algorithms and applications, IEEE Signal processing Magazine, July 2001.
- [3] Jiang Xuehua, —Digital Watermarking and Its Application in Image Copyright Protection, 2010 International Conference on Intelligent Computation Technology and Automation.
- [4] Ensaf Hussein, Mohamed A. Belal, —Digital Watermarking Techniques, Applications and Attacks Applied to Digital Media: A Survey, IJERT, ISSN: 2278-0118, Vol. 1 Issue 7, September-2012.
- [5] C.-T. Li and F.M. Yang., —One-dimensional Neighborhood Forming Strategy for Fragile Watermarking. In Journal of Electronic Imaging, vol. 12, no. 2, pp. 284-291, 2003.
- [6] Rakesh Ahuja, S S Bedi, Himanshu Agarwal, —A Survey of Digital Watermarking Schemes, MIT International Journal of Computer Science and Information Technology, Vol.2, No. 1, Jan. 2012, pp.(52-59)
- [7] G. Coatrieux, L. Lecornu, Members, IEEE, Ch. Roux, Fellow, IEEE, B. Sankur, Member, IEEE, IAA Review of digital image watermarking in health care.
- [8] Edin Muharemagic and Borko Furht —A Survey of watermarking techniques and applications, 2001.
- [9] Jahnvi Sen, A.M. Sen, K. Hemachandran, AN ALGORITHM
- [10] Vidyasagar M. Potdar, Song Han, Elizabeth Chang, —A Survey of Digital Image Watermarking Techniques, 2005 3rd IEEE International conference on Industrial Informatics (INDIN).
- [11] Evelyn Brannock, Michael Weeks, Robert Harrison, Computer Science Department Georgia State University —Watermarking with Wavelets: Simplicity Leads to Robustness, Southeast on, IEEE, pages 587 – 592, 3-6 April 2008.
- [12] Cox, I.J.; Miller, M.L.; Bloom, J.A., —Digital Watermarking, Morgan Kaufmann, 2001.
- [13] Sunil Sharma1, Mahendra Kumar Rai2 and Tanvi Sharma, “An Enhance LSB Watermark Approach for Robustness and Security in uncompressed AVI Video,” International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 3, Issue 1, January –February 2014
- [14] Sunil Sharma, Mahendra Kumar Rai, “An Enhance Video Watermarking approach for robustness and security using Pixel and Transform Domain in an uncompress AVI video, International Journal for Research in Applied Science and Engineering Technology (IJRASET), Vol. 2 Issue VI, June 2014.
- [15] Tanvi Chauhan, Prof. Vineet Richhariya, Sunil Sharma, “Literature Report on Face Detection with Skin & Reorganization using Genetic Algorithm”, Tanvi Chauhan et al. / IJAIIR Vol. 2 Issue 2 ISSN: 2278-7844
- [16] Aanchal Chauhan, Zuber Farooqui, “AN INVENTIVE APPROACH FOR FACE DETECTION WITH SKIN SEGMENTATION AND MULTI-SCALE COLOR RESTORATION TECHNIQUE USING GENETIC ALGORITHM”, INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTERAPPLICATIONS AND ROBOTICS, Vol. 4 Issue 1, January 2016
- [17] Tanvi Chauhan, Vineet Richhariya, “Real Time Face Detection with Skin and Feature Based Approach and Reorganization using Genetic Algorithm”, CIIT Digital Image Processing, Vol 5, No 1 (2013)
- [18] S R Tandan, Niharika Vaishnav, “A Bird's Eye View of Anti-Phishing Techniques for Classification of Phishing E-Mails” International Journal for Research in Applied Science & Engineering, Technology (IJRASET) (2015)
- [19] Gaurav Kumar Rai, Rohit Miri, S R Tandan “Enhanced Security Technique in WAP & WEP Based Wireless (Wi-Fi) Network for the Protection against Unauthorized Users international journal for advance research in engineering and technology (ijaet), (2014)
- [20] Niharika Vaishnav, S R Tandan “Development of Anti Phishing Model for Classification of Phishing E-Mail” International Journal of Advanced Research in Computer and Communication Engineering, (2015).
- [21] G Singhal, S R Tandan, R Miri “IAA (Internet access account) based security modal for detection and prevention of cyber crime” International Journal of Engineering Research and Technology, (2013)
- [22] Shikha Gupta, S R Tandan, R Miri “Modeling of Election Algorithm for Coordinator Selection Using Neuro Fuzzy Approach in Distributed Computing Environment” International Journal of Engineering Research and Technology, (IJERT), (2013)

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

- [23] K Lahre, S R Tandan, R Miri "Implementation of Improved Distributed Wireless Channel Allocation Algorithm for Mobile Computing" Wireless Communication-CIIT-IJ, (2011)
- [24] Amit Dewangan, Sadaf Rahman, "Secured Wireless Content Transmission over Cloud with Intelligibility" International Journal of Engineering and Applied Sciences (IJEAS) ISSN: 2394-3661, Volume-2, Issue-5, May 2015.



10.22214/IJRASET



45.98



IMPACT FACTOR:
7.129



IMPACT FACTOR:
7.429



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089  (24*7 Support on Whatsapp)