OVERVIEW OF DIGITAL IMAGE WATERMARKING WITH COMPARATIVE ANALYSIS OF DIFFERENT TECHNIQUES

Shishank shrivastava[1], Mahendra Kumar Pandey[2]
Research Scholar, Dept. of Electronics and Communication Engineering, RJIT, Gwalior, INDIA
Assistant Professor, Dept. of Electronics and Communication Engineering, RJIT, Gwalior, INDIA

Abstract: Information security is extremely significant concern for the internet technology. As most of the data available in digital form, the multimedia owners need to protect their data from their unauthorized use. The protection of intellectual property rights has become increasingly important. These concerns over protecting copyright have triggered significant research to find ways to hide copyright messages and serial number into digital media. An important sub discipline of information hiding is Watermarking. Digital Watermarking is an authentication technique which permanently embeds a digital signal (watermark) in text, image, audio, video files (any Data) by slightly modifying the data but in such a way that there are no harmful effects on the data. In this paper, a review analysis of different watermarking techniques has been presented. Here, we elaborate the most important digital image watermarking methods and focus the merits and demerits of these techniques. Analysis has been exploring the performance efficiency of various digital image watermarking techniques that compared on the basis of outputs.

Keywords — Digital Watermarking; Data Security; Discrete Cosine Transform; Discrete Wavelet Transform

1. INTRODUCTION

In recent years, digitization play big role in human life as numerous applications in field of engineering, healthcare, communication, documentation and many more. Therefore, authentication, information security and other various issues are raised with multimedia sources and content. Digital data can be stored efficiently and with a very high quality, and it can be manipulated very easily using Computers. Furthermore, digital data can be transmitted in a fast and inexpensive way through data communication networks without losing quality. Digital media offer several distinct advantages over analog media. The quality of digital audio, images and video signals are better than that of their analog counterparts. Editing is easy because one can access the exact discrete locations that need to be changed. Copying is simple with no loss of fidelity and a copy of a digital media is identical to the original [1-3]. The above problem can be solved by hiding some ownership data into the multimedia data, which can be extracted later to prove the ownership. This idea is implemented in bank currency notes. In bank currency notes, a watermark is embedded which is used to check the originality of the note. The same "watermarking" concept may be used in multimedia digital contents for checking the authenticity of the original content [4-5]. So, A Watermarking is adding "ownership" information in multimedia contents to prove the authenticity. This technology embeds a data, an unperceivable digital code, namely the watermark, carrying information about the copyright status of the work to be protected. Continuous efforts are being made to device an efficient watermarking schema but techniques proposed so far do not seem to be robust to all possible attacks and multimedia data processing operations. Considering the enormous financial implications of copyright protection, there is a need to establish a globally accepted watermarking technique. The sudden increase in watermarking interest is most likely due to the increase in concern over IPR. Today, digital data security covers such topics as access control, authentication, and copyright protection for still images, audio, video, and multimedia products. A pirate tries either to remove a watermark to violate a copyright or to cast the same watermark, after altering the data, to forge the proof of authenticity [1-6].

The manuscript followed by the overview of image watermarking, survey of watermarking scheme, comparison and concluding remarks in respective section.

2. OVERVIEW OF WATERMARKING

Digital Watermarking is an authentication technique which permanently embeds a digital signal (watermark) in text, image, audio, video files (any Data) by slightly modifying the data but in such a way that there are no harmful effects on the data. The watermark embedded may contain information such as identification of the product's owner, user's license information etc. This watermark can then be detected whenever required to identify its owner or to check whether a user is authentic to access that data or no. Digital Watermarking used as hiding of facts. It is an invisible signature picture to reveal authenticity and ownership. It is better than cryptography and stenography because it can protect content even after it is decrypted. DW schemes have two domains, namely spatial domain and transform (frequency) domain. In spatial domain (SD) technique, the watermark bits are embedded without delay into the pixels of cover image (CI). In Transform domain (TD), the watermark is embedded by way of converting the coefficient magnitude in a TD using discrete cosine transform (DCT), discrete wavelet transform (DWT), and singular value decomposition (SVD) technique. In digital watermarking there are mainly two images i.e. cover image and watermark image. With these 2 pictures DW has procedures: Embedding Process and Extraction Process.

Embedding Process: In which the watermark is embedded in the original image i.e. CI by using the embedding algorithm. Then the watermarked image (WI) is generated. So the WI is transmitted over the network.

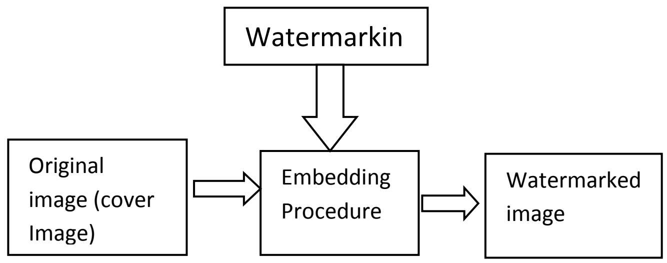

Fig. 1. Embedding Process

Extraction Process: In this system, the watermark is detected or extracted by the dedicated detector from the WI by making use of a few extraction set of rules. In addition to this, noise is also detected.

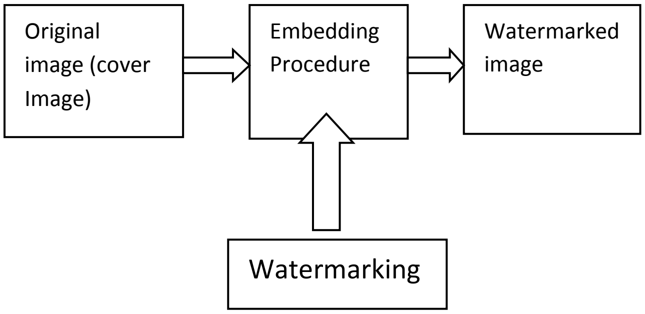

Fig. 2. xtraction Process

A watermark is designed to permanently reside in the host data and needs to satisfy the following conditions:-

- Imperceptible, so that it doesn't cause any interference.
- Statistically undetectable to ensure security.
- Cannot be removed or modified by any signal processing operation (*e.g.* filtering, compression, MP3-encoding, etc) without degrading perceptual quality.

Image watermarking is very emerging technology to protect the images from unauthorized owner. There are several properties are present to determine the quality of watermarking scheme such as robustness, Imperceptibility, capacity and blind watermarking [1-17]. These properties may vary with different application of watermarking. Therefore, watermarking schemes are classified as per these properties and different application as discussed below.

2.1 Types of Image Watermarking

*Visible watermark***:** *Visible watermarking*

In this method the embedded watermark is visible to the stop user. It is the sooner method of watermarking. The watermark is embedded on the cover page of the picture. It is the primary approach of watermarking tried for the cause of protection. It is embedded in this kind of manner that it's miles surely seen via the naked eyes to the person. In this watermark is added at the CI. In this way watermark is visible to the cease person certainly.

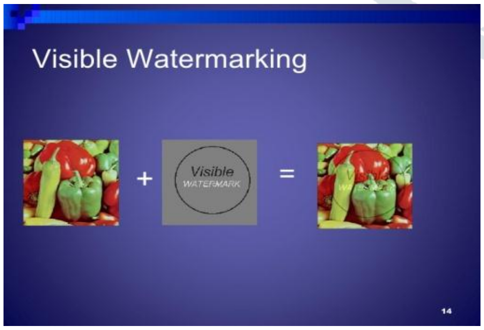

Fig. 3. Visible watermarking

*Invisible Watermark***:** It is that sort of watermarking approach in which embedded watermark is not visible to the viewer. In this the delivered watermark at the digital information cannot be understand. The watermark is embedded at the overlaid picture. This watermark is not visible to the end user but still it can be detected by using algorithms or various techniques. In this watermark is digitally embedded in the image. These kinds of watermarks are used to proof the ownership. It is also used to detect the misuse of the product. It is too measured as the backup for visible watermarking [2].

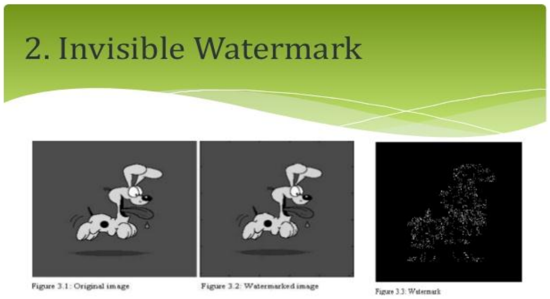

Fig. 4. Invisible Watermarking

Fig. 5.

Robust Watermark: Robustness watermarking scheme is used for sign copyright information of the digital works, the embedded watermark can resist the common edit processing and various attacks.

Fragile Watermark: Fragile watermarking is mainly used for integrity protection, which must be very sensitive to the changes of signal. It can be determine whether the data has been tampered according to the state of fragile watermarking.

Semi fragile Watermark: Semi fragile watermarking is capable of tolerating some degree of the change to a watermarked image, such as the addition of quantization noise compression attacks.

Invisible-Robust Watermark: The invisible-robust watermark is embedding in such a way that processes made to the pixel level; which are perceptually not determine and it can be recovered only with appropriate decoding process.

Invisible-Fragile Watermark: The invisible-fragile watermark is embedded in such a way that any attacks of the image would alter or destroy the watermark.

2.2 Application of Image Watermarking

Digital image watermarking is a very active research field with a lot of applications. Although it is a relatively new field, it has produced important algorithms for hiding messages into digital signals. The increasing amount of research on watermarking over the past decade has been largely driven by its important applications in digital copyrights management and protection. There are several different application area also exploited for watermarking benefits such as copyright protection, digital right management, tamper proofing, broadcasting monitoring, fingerprinting, access control, medical application, image and content authentication. These are discussed below [1, 4-5].

Copyright protection: Digital image watermarking can be used to identify and protect copyright ownership as well as illegally replicated.

Digital right management: watermarking scheme can protect the digital rights such as identification, trading, protecting, monitoring, and tracking of all forms of usages over tangible and intangible assets.

Tamper proofing: Digital watermarks which are fragile in nature, can be used for tamper proofing. Digital content such as image, audio, video 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.

Broadcast monitoring: watermarking can protect the content ownership during the broadcasting of information over the telephone line, TV or internet etc.

Fingerprinting: 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.

Access control: 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 to allow access with control capacity.

Image and content authentication: a watermark can proof the image or content are authentic or not based on embedded watermark.

Therefore, various application and advantages are present of image watermarking. In this context, several methods are developed over the past decade based different techniques particular transform based watermarking schemes are shown their robustness in term of properties in different application.

3. ATTRIBUTES OF DIGITAL IMAGE WATERMARKING

The necessities for image watermarking (IW) can be handled as traits, properties or attributes of IW. Different applications call for unique residences of watermarking. Requirements of IW range and outcome in various layout troubles relying on picture watermarking programs and motive. These requirements need to be taken into consideration at the same time as designing watermarking device. There are simple 5 requirements as follows [4].

3.1 Fidelity

It may be taken into consideration as a measure of perceptual transparency or imperceptibility of watermark. It refers to the similarity of un-watermarked and WI. This angle of watermarking exploits trouble of human vision. Watermarking should not introduce seen distortions as it reduces commercial value of the WI.

3.2 Robustness

Watermarks must now not be removed deliberately or by accident by simple IP operations Hence watermarks should be robust towards variety of such attacks. Robust watermarks are designed to resist everyday processing. On the other hand, fragile watermarks are designed to convey any attempt to exchange digital content.

3.3 Data Payload

Data payload is also known as capacity of watermarking. It is the maximum quantity of records that can be hidden without degrading image satisfactory. It can be evaluated by way of the quantity of hidden information. This belonging describes how lot information has to be embedded as a watermark so that it is able to be successfully detected at some stage in extraction.

3.4 Security

Secret key has for use for embedding and detection manner in case security is a primary situation. There are 3 forms of keys utilized in watermark systems: public-key, detection-key and public-key. Hackers should not be able to remove watermark with anti-reverse engineering research algorithm. 3.5 Computational Complexity

Computational complexity suggests the amount of time watermarking set of rules takes to encode and decode. To make sure security and validity of watermark, extra computational complexity is wanted. Conversely, actual-time applications necessitate both pace and performance.

4. PROBLEMS IN PREVIOUS RESEARCH

In the field of DW, DIW has attracted a lot of attention in the research community for two reasons: one is its easy availability and the other is that it conveys enough redundant information that could be used to embed watermarks. DW incorporates diverse strategies for protective the virtual content. The whole DIW strategies always work in domains either SD or TD. The SD techniques works at once on pixels. It embeds the watermark by using enhancing the pixels cost. Most normally used SD strategies are LSB. TD techniques embed the watermark by modifying the TD coefficients. Most usually used TD method is DCT and DWT. The SD watermarking is simple as compared to the TD watermarking. The robustness is the main limitation of the SD watermarking. It can live on easy operations like cropping and addition of noise. Another dilemma of SD method is they do now not allow for the subsequent processing for you to increase the robustness of watermark. Basically there are mainly 3 challenges being faced by the currently available Watermarking schemes and those challenges are:

1) Time Complexity
2) Quality Complexity
3) Watermarking Standards

Here according to these challenges first one increase the algorithm latency which in turn will increase the complexity in hardware unit and will also result in more power consumption. Now about quality complexity sometimes due to watermarking the original quality of image is changed which becomes a crucial problem for any application. Third one is watermarking standard this challenge is being faced when watermarking level does not suffice with its encryption levels. Hence these three are the main challenges which are to address and are being faced by the previous and existing works.

5. LITERATURE SURVEY

In recent years, digital media are gaining wider popularity due to their security related issues are becoming greater concern. Digital watermarking is a technique which allows an individual to add copyright notices or other verification messages to digital media. The transform domain watermarking is achieving very much attention and success as compared other contemporary watermarking schemes. Transform-domain watermarking techniques are typically much more robust to image manipulation compared to the spatial domain techniques. This is because the transform domain does not use the original image for embedding the watermark data. In addition, a transform domain algorithm spreads the watermark data over all part of the image. Additionally, frequency domain-based techniques can embed more bits for watermark and are more robust to attack. There are most commonly used transform domain methods is Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT). This technique discussed in brief in listed literature references which describes the previous work which had been done on digital watermarking by using DWT technique and other techniques, including the analysis of various watermarking schemes and their results.

Mistry [6] introduced digital watermarking methods-Spatial domain (like LSB) and transform domain (like DCT, DWT) methods. The spatial domain is the normal image space, in which a change in position in image directly projects to a change in position in space. Ex.-Least Significant bit (LSB) method. Transform Domain Method produce high quality watermarked image by first transforming the original image into the frequency domain by the use of Fourier Transform, Discrete Cosine Transform (DCT) or Discrete Wavelet transforms (DWT). Authors found that transform watermarking is comparatively much better than the spatial domain encoding.

Van et al. [7] proposed two LSB techniques. First replaces the LSB of the image with a pseudo-noise (PN) sequence, while the second adds a PN sequence to the LSB of the data. Another LSB data hiding method called Patchwork chooses n pairs (ai; bi) of the points in an image and increases the brightness of the ai by one unit while simultaneously decreasing the brightness of bi. The problem with this paper is that data is highly sensitive to noise and is easily destroyed. Furthermore, image quality may be degraded by the watermark.

Blossom et al. [8] proposed a DCT based watermarking scheme which provides higher resistance to image processing attacks such as JPEG compression, noise, rotation, translation etc. In this approach, the watermark is embedded in the mid frequency band of the DCT blocks carrying low frequency components and the high frequency sub band components remain unused. Watermark is inserted by adjusting the DCT coefficients of the image and by using the private key. Watermark can then be extracted using the same private key without resorting to the original image. Performance analysis shows that the watermark is robust.

W. Hong et al. [9] proposed a robust digital watermarking scheme for copyright protection of digital images based on sub-sampling. The watermark is a binary image, which is embedded in discrete transform coefficient of the host image and not used in the original image. In this scheme, they had used chaotic map in watermarked image. However the result of watermark image is good and robust to attack.

Xia et.al [10] proposed a watermarking scheme based on the Discrete Wavelet Transform (DWT). The watermark, modeled as Gaussian noise, was added to the middle and high frequency bands of the image. The decoding process involved taking the DWT of a potentially marked image. Sections of the watermark were extracted and correlated with sections of the original watermark. If the cross-correlation was above a threshold, then the watermark was detected. Otherwise, the image was decomposed into finer and finer bands until the entire, extracted watermark was correlated with the entire, original watermark. Performance analysis shows that DWT is more robust to attack than DCT. The problem with the proposed method is that this technique is susceptible to geometric attacks.

Akhil et al. [11] proposed a robust image watermarking technique based on 1-level DWT (Discrete Wavelet Transform). This method embeds invisible watermark into salient features of the original image using alpha blending technique. Experiment result shows that the embedding and extraction of watermark is depend only on the value of alpha. All the results obtained for the recovered images and watermark is identical to the original images.

G. Bhatnagar et al. [12], presented a semi-blind reference watermarking scheme based on discrete wavelet transform (DWT) and singular value decomposition (SVD) for copyright protection and authenticity. Their watermark was a gray scale logo image. For watermark embedding, their algorithm transformed the original image into wavelet domain and a reference sub-image is formed using directive contrast and wavelet coefficients. Then, their algorithm embedded the watermark into reference image by modifying the singular values of reference image using the singular values of the watermark.

M. Barni et al. [13] have developed an improved wavelet-based watermarking through pixel-wise masking. It is based on masking watermark according to characteristics of HVS. The watermark is adaptively added to the largest detail bands. The watermark weighing function is calculated as a simple product of data extracted from HVS model. The watermark is detected by correlation. The proposed method is robust to various attacks but this method is complex than other transform technique.

Chitla Arathi et al.[14] presented a watermarking technique based on block based SVD(singular value decomposition).Semi-fragile watermark is fragile to malicious modifications while robust to incidental manipulations .The scheme can extract the watermark without the original image. SVD transformation preserves both one-way and non-symmetric properties that are not obtainable in DCT and DFT transformations. This technique can also detect tamper made on the image.

Madhuri Rajawat [15], presents digital watermarking for their applications, techniques, attacks, classifications and tempering detection. With the help of these techniques they improve the security of image. This paper worked on RGB components such as red, green, blue for enhancing robustness and security. 2-DWT applied on RGB components for good results. The author concluded that tampering detection and watermarking method is very important for protection against attacks.

Arash Saboori [16], presents a new method is proposed using the combination of DCT and PCA transform in order to reduce the low frequency band for the color image in YUV color space. The Y (luminance) is divided into non-overlapping blocks and the low band coefficients of each block are placed in the matrix data than PCA transform are applied on it. This method eliminates the disadvantage of low band based on the combination of DCT and PCA transform.

D. Vaishnavi [17] Introduce two methods for invisible and robust watermarking proposed in RGB color space. In the first method, gray scale watermark is embedded on the blue color channel and in second method, blue color watermark is embedded on the blue color channel element after which SVD applied at the blue channel of host photograph to retrieve singular values. They concluded that first method gives a good robustness for median filtering attacks, for motion blur etc. and second method gives good robustness for Gaussian noise, salt-pepper noise etc.

6. COMPARISON OF VARIOUS IMAGE WATERMARKING TECHNIQUES

The frequency sensitivity refers to the attention’s response to spatial, spectral, or time frequency adjusts. Spatial frequencies are perceived as styles or textures, and spatial frequency sensitivity is generally defined as the attention’s sensitivity to luminance modifications. It has been shown that an eye fixed is the maximum touchy to luminance changes inside the mid-range spatial frequencies, and that sensitivity decreases at lower and higher spatial frequencies. DIW schemes particularly fall into two wide categories:

- Spatial-domain techniques.
- Frequency-domain techniques.

5.1 Spatial Domain Techniques

Spatial watermarking also can be implemented the use of coloration separation. In this way, the watermark appears in most effective one of the shade bands. This renders the watermark visibly subtle such that it's miles difficult to locate below regular viewing. However, the mark appears immediately when the colors are separated for printing. This renders the file useless for the printer; the watermark can be eliminated from the color band. This manner is used commercially for reporters to look into digital photos from a image-stock house before shopping for unmarked variations.

5.2 Frequency Domain Techniques

Compared to SD strategies, frequency-domain methods are more extensively implemented. The intention is to embed the watermarks inside the spectral coefficients of the image. The most commonly used transforms are the DCT, DFT, DWT, The cause for watermarking within the frequency area is that the characteristics of the human visual system (HVS) are higher captured through the spectral coefficients. For example, the HVS is more sensitive to low frequency coefficients, and less sensitive to high-frequency coefficients. In other words, low frequency coefficients are perceptually extensive; because of this changes to the ones additives would possibly motive distortion to the authentic picture. On the alternative hand, high-frequency coefficients are considered insignificant; for that reason, processing techniques, which include compression, have a tendency to cast off excessive-frequency coefficients aggressively. To acquire a balance among imperceptibility and robustness, most algorithms embed watermarks in the midrange frequencies.

TABLE I. COMPARISONS OF DIFFERENT WATERMARKING TECHNIQUES

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

7. CONCLUSION

An overview of image watermarking techniques is presented, which is applicable for various applications such as multimedia security as well as secure communication of multimedia data. These techniques are work as hidden watermark mostly. In literature, several techniques are presented. These techniques have good efficiency of robust watermarking as well as watermark extraction and also provide a consistent robust performance on different original image and watermarked image using various techniques as presented in reported literature.

8. REFERENCES

[1] W. Bender, D. Gruhl, N. Morimoto and A. Lu, "Techniques for Data Hiding," IBM System Journal, vol. 35, NOS 3&4, pp. 313-336, 1996.

[2] E. T. Lin and E. J. Delp, "A Review of Data Hiding in Digital Images," in Proc. of the Image Processing, Image Quality, Image Capture Systems Conf. (PICS' 99), pp. 274-278, Apr. 1999.

[3] P. H. W. Wong, O. C. Au and G. Y. M. Yeung, "A Novel Blind Multiple Watermarking Technique for Images," accepted by IEEE Transactions on Circuits and Systems for Video Technology: Special Issue on Authentication, Copyright Protection and Information Hiding, Sept. 2003.

[4] Mr. Gaurav N Mehta, Mr. Yash Kshirsagar, Mr. Amish Tankariya," Digital Image Watermarking: A Review", International Journal of Scientific Engineering and Technology (ISSN : 2277-1581) www.ijset.com, Volume No.1, Issue No.2 pg:169-174 01 April 2012.

[5] Singh A. P., Mishra A., Wavelet Based Watermarking on Digital Image, Indian Journal of computer Science and Engineering 2011.

[6] Darshana Mistry, Comparison of Digital Watermarking methods, 21st Computer Science Seminar SA1-T1-7, IJCSE, 2010.

[7] R. G. van Schyndel, A. Z. Tirkel, and C. F. Osborne, A digital watermark, in Proc. IEEE Int.Conf. Image Processing (ICIP), 1994.

[8] BlossomKaur,AmandeepKaur, Jasdeep Singh,Steganographic Approach for hiding Image in DCT Domain, International Journal of Advances in Engineering & Technology, July 2011.

[9] W. Hong and M. Hang, Robust Digital Watermarking Scheme for Copy Right Protection,IEEE Trans. Signal Process, vo.l2, pp. 1-8, 2006.

[10] X. Xia, C. Boncelet, and G. Arce, A Multiresolution Watermark for Digital Images,Proc. IEEE Int. Conf. on Image Processing, Oct.1997.

[11] Akhil Pratap Shing, Agya Mishra, Wavelet Based Watermarking on Digital Image, Indian Journal of computer Science and Engineering, 2011.

[12] Bhatnagar, G. and Raman, B., A new robust reference watermarking scheme based on DWTSVD,Elsevier B.V. All rights reserved, 2008.

[13] Barni M, Bartolini F, Piva, An Improved Wavelet Based Watermarking Through Pixelwise Masking,IEEE transactions on image processing, 2001.

[14] ChitlaArathi,'' A Semi Fragile Image Watermarking Technique Using Block Based SVD",International Journal of Computer Science and Information Technologies, Vol. 3 (2), 2012.

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

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

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