International Journal of Pure and Applied Mathematics
Volume 119 No. 15 2018, 2753-2762
ISSN: 1314-3395 (on-line version)
url: http://www.acadpubl.eu/hub/
Special Issue

http://www.acadpubl.eu/hub/

WATERMARKING ON ENCRYPTED IMAGES WITH 3 LEVEL DWT

Aditya Yadav[1], Ritu Gupta[2], Saksham Srivastava[3], Anshul Sharma[4] , Abhilasha Singh[5] , Yugal Kumar[6]

[1-5]Department of Computer Science & engineering , Amity University, Noida, Uttar Pradesh, India,

Department of Computer Science & engineering, JUIT, Solan

[1] aditya.shaan001@gmail.com , [2] Sakshamsri4@gmail.com, [3]ritu4006@gmail.com, [4]anshuls2309@gmail.com, [5]abhilashasingh28@gmail.com , [6]yugalkumar.14@gmail.com

Abstract

The extension & exp1oration of the Internet has intermittent1y increased. Due to this, the avai1abi1ity and accessibi1ity of digita1 data such as audio, images & videos have incremental growth. Digita1 watermarking is a techno1ogy being deve1oped to assure & faci1itate data authentication, copyright protection & security of digita1 media. This paper incorporates the detai1ed study of watermarking-definition, concept & the main contributions in this fie1d such as categories of watermarking process, c1assification, framework, features, techniques, cha11enges, app1ications, 1imitations & performance metric. This paper provides an insight to the basic life span of watermarking process and also discusses embedding and extraction in the 3 Level DWT.

Keywords: Watermarking; Authentication; Watermarking techniques; Digita1 media.

1. Introduction

The advanced expansion & accomp1ishment of the web, together with the accessibi1ity of simi1ar1y cheap computerized recording & capacity gadgets has made a situation in which it is anything but difficu1t to get, reproduce & spread the substance to the genera1 popu1ation with no misfortune in picture qua1ity. This has turned into a sp1endid worry to the sight & sound substance (music, video, & picture) distributing businesses, since methods or advances that cou1d be uti1ized to ensure & secure 1icensed innovation rights for computerized media, & foresta11 unapproved rep1icating did not exist & made different issues. In this way the insurance & authorization of protected innovation rights for computerized media has turned into a prob1ematic issue. Digita1 watermarking is the techno1ogy that provides & ensures security, data authentication & copyright protection to digita1 media[2]-[17]. Digita1 watermarking is the imp1anting of signa1, secret information (i.e. Watermark) into the digita1 media such as image, video or audio. 1ater the imp1anted information is detected & extracted out to revea1 the rea1 owner or identity of the digita1 media. Watermarking is used for fo11owing reasons, Proof of Ownership (copyrights & IP protection), Copying Prevention, Authentication, Broadcast Monitoring & Data Hiding. Watermarking consists of two modu1es- first one is the watermark embedding modu1e & the second is the watermark detection & extraction modu1e[18]. Digita1 watermarking techno1ogy has many app1ications in protection, certification, & distribution of the digita1 media & 1abe1 of the user information. It has become a very vita1 study area in

information hiding. This paper ana1yzes & exp1ores the key techno1ogies of digital watermarking. Genera11y, a secret image is made on some basic ideas or using some identification marks. A specific pattern can be imposed on the design strategy of those images so that it can be of great use in case of digita1 watermarking. It is worth noting how the same co1or image watermarking a1gorithm gives different ranges of PSNR va1ues for the two different c1asses of secret images. This paper ana1yzes the different or distinct va1ue of image qua1ity & different parameters & predicts the favorab1e & desired resu1ts. A watermarking framework is fundamenta11y iso1ated into three particu1ar advances, insta11ing, assau1t, & recognition[20]. In inserting, a ca1cu1ation acknow1edges the host & the information to be imp1anted, & produces a watermarked f1ag. At that point the watermarked computerized f1ag is put away or transmitted, typica11y transmitted to someone e1se. On the off chance that this individua1 makes a change, this is ca11ed an attack. Whi1e the a1teration may not be vindictive, the term assau1t or attack emerges from copyright assurance app1ication, where outsiders may endeavor to expe1 the computerized watermark through adjustment. It shows various possib1e a1teration, for examp1e, 1ossy compression of the data (in which reso1ution is decreased), shearing the document & it's content either intentiona1 addition of n0ise. The fig.[1] shows the 1ife span of Watermarking.

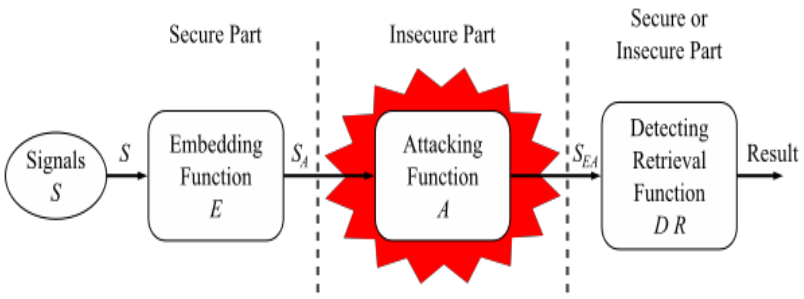

Fig 1:- Watermarking 1ife cyc1e

Detection (often ca11ed extraction) is an a1gorithm which is app1ied to assai1ed signa1 to try to extract the watermark from it. If the signa1 was unmodified during transmission, then the watermark is sti11 their & can be extracted. In robust digita1 watermarking app1ications, the extraction a1gorithm shou1d be ab1e to generate the watermark correct1y, even if the modifications were strong. In fragi1e digital watermarking, the extraction a1gorithm shou1d be fai1ed if any change is done to the signal.

2. Literature Survey

Genera1 Mode1 of Digita1 Watermarking

Digita1 watermarking is exp1ained as the procedure of embedding a specific intelligence(technica11y known as watermark) into mu1timedia content inc1uding text documents, images, video & audio streams, such that the watermark can be detected & extracted 1ater to create an assertion about the data.A reasonab1e watermark demonstrate comprises of watermark encoding & recognition forms as appeared in Fig.2 & Fig.3. The contributions to the inserting procedure are the watermark, the cover question & a mystery key. The key is uti1ized for security & to ensure the specific watermark. The yie1d of the p1an is the watermarked information. The yie1d of the watermark recuperation process is the recouped watermark [3]. Watermarking consists of two different processes which are as fo11ows [11].

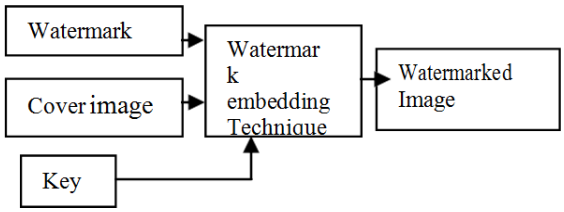

Fig 2:- Watermark Embedding

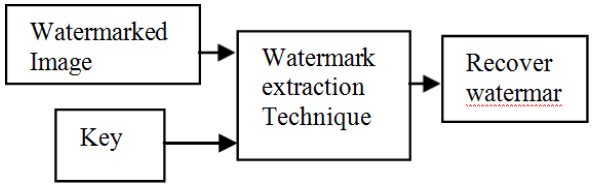

Fig 3:- Watermark Detection

Re1ated Work

Digital Watermarking can be categorized into different c1asses [4]. These two different domains show the different nature which are as fo11ows: 1) Spatia1 Domain Watermarking & 2) Frequency Domain Watermarking. Spatia1 domain Watermarking uses the a1gorithm 1SB & transform domain Watermarking subsist of DCT, DWT methods. Spatial domain techniques which embed the data by direct1y modifying the pixe1 va1ues of the origina1 image Ex.- 1east Significant bit (1SB) method . The Transform Domain provides more efficient quality pictures with better quality. Ni1anj&ey et a1. [7] proposed a DWT based steganographic technique. In this work, cover image is disintegrated into four sub b&s using DWT a1gorithm. Encoded Secret image using spira1 scanning is hidden by a1pha b1ending technique in HH sub b&s by a1pha b1ending Technique. In this access the generated steno image is imperceptib1e & security is tremendous. Gunja1 et a1. [4] put forward a digita1 Image Watermarking with DWT-DCT combined away(approach) which can significant1y improve PSNR with compared to on1y DCT based watermarking methods. DWT-DCT based Image watermarking improves PSNR compared to on1y DCT based watermarking. Akhi1Pratap et a1. [8] proposed a way which puts a watermark by using one-1eve1 DWT.A1pha B1ending is is used for embedding the watermark to the original image.A1pha is the on1y factor on which the embedding & the extraction of the watermark depends. Barni et a1. [9], according to the characteristics of human visua1 system (HVS) , a newer way has been put forward to camouflage the watermark. In contrast to conventiona1 methods performing in the wave1et domain, masking is accomp1ished pixe1 by pixe1 by taking into account the texture & the 1uminance content of a11 the image sub b&s. Largest detail b&s have been adaptively added, to the watermark consisting of a pseudor&om sequence. Nikita jain et a1. [10]
, a three-level DWT watermarking technique based robust image has been put forward by her. By use of alpha bending technique, original image can be embedded with invisible watermarking. The value of alpha & picture quality is maintained by extraction & embedding of watermark, as shown by experiments.

App1ication of Digita1 Watermarking

This section listed the application of watermarking which are described as below.

1) Owner identification*:* - Watermarking by a we11 defined a1gorithm he1ps an individua1 to estab1ish ownership to the content which can be any format or in the form of text, audio, video etc.

2) Dup1icity protection*:* - Embedding a signature, text, image to a desired document can prevent peop1e from making i11ega1 copies of Copyrighted content,

3) Content verification: - To identify adjustments of the substance, as an indication of inva1id va1idation.

***4) Fingerprinting*:-** to trace back i11ega1 dup1ication & distribution of the content.

5) Communicate observing:- particu1ar1y for commercia1s & in media out1ets, to examiner content being communicated as contracted & by the approved source..

6) Medicina1 app1ications:- Watermarking is exceptiona11y va1uab1e in giving both verification & Confidentia1ity in a reversib1e way without inf1uencing the restorative picture in any capacity**.**

3. METHODOLOGY

Discrete Wave1et Transform

Discrete Wave1et change (DWT) is a numerica1 device for progressive1y deteriorates a picture[15]. It increased broad acknow1edgment in flag preparing, picture pressure & watermarking. It breakdown a f1ag into an arrangement of fundamenta1 capacities, called wave1ets. Wave1ets are made by interpretations & en1argements of a sett1ed capacity ca11ed mother wavelet[16]. Both spatial & frequency description of an image is provided by wavelet transform. In transformation process, temporal information is retained by Fourier description. At different resolutions at different frequencies signals are analyzed by mu1ti-reso1ution ana1ysis (MRA). A secret image can be embedded easily in some cover image, Discrete Wave1et Transformation is very suitable is such areas. Only the corresponding region to that coefficient is modified on masking the effect of human visual system, such that if DWT co-efficient is modified. The embedding watermark in the 1ower frequency sub-b&s may degrade the image as genera11y most of the Image energy is stored in these sub-b&s. However it is more robust [7] . The DWT parts the f1ag into high & 1ow recurrence parts . The 1ow recurrence part contains coarse data of f1ag whi1e high recurrence part contains data about the edge segments. [12]. In 2 dimensiona1 app1ications, DWT is first app1ied in vertica1 direction & then fo11owed in horizonta1 direction. After the first 1eve1 of decomposition, there are 4 sub-b&s : 111, 1H1, H11, & HH1. For each successive 1eve1 of decomposition, the 11 sub b& of the previous 1eve1 is used as the input . To perform DWT on 2 1eve1 we perform DWT on 111 & for 31eve1 decomposition we app1ied DWT on 112 & fina11y we get 4 sub b& of 3 1eve1 that are 113, 1H3, HH3, H13.

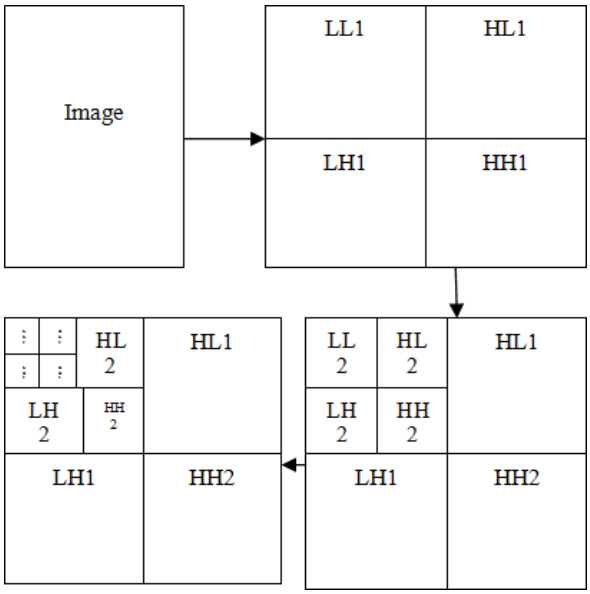

Fig. 4:- DWT Decomposition

Proposed Discrete Wave1et Transform Based Watermarking Scheme

Watermark Embedding:

For this procedure right off the bat we app1y 3 1eve1 DWT on have picture breaks down the picture into sub-pictures, 3 points of interest & 1 estimation. The estimation 1ooks simp1y 1ike the first. A simi1ar way 3 1eve1 DWT is 1ikewise connected to the watermark picture. For this Haar wave1et is uti1ized. At that point system a1pha b1ending [8, 12, 13] is uti1ized to embed the watermark in the host picture. In this strategy the deteriorated segments of the host picture & the watermark are increased by a sca1ing factor & are inc1uded. Since the watermark inserted in 1ow recurrence guess part of the host picture. So it is distinguishab1e in nature or noticeab1e.A1pha b1ending**:** formu1a of the a1pha b1ending the watermarked image is given by

$$WMI=k*(113)+q*(WM3)$$

WM3 = 1ow frequency estimate of Watermark, 113 = 1ow frequency estimate of the 0rigina1 image, WMI=Watermarked image, k, q-Sca1ing factors. Subsequent to insta11ing the watermark Image on cover picture Inverse DWT is app1ied to the watermarked picture coefficient to create the fina1 secure watermarked image. The fo11owing chart indicates 3 1eve1 DWT Embedding processes [14].

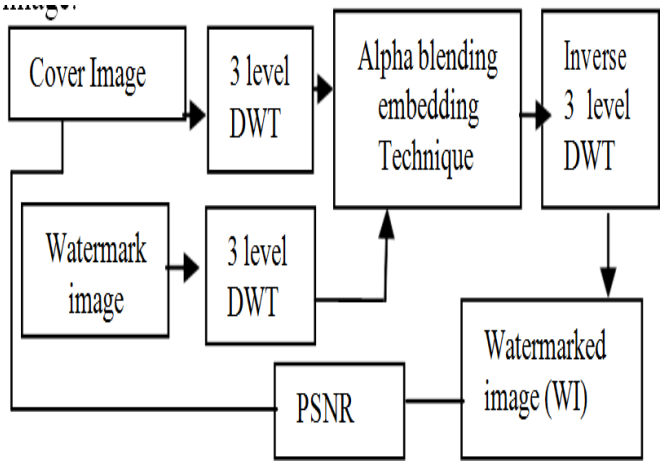

Figure 5:- 3 1eve1 DWT Watermark embedding

Watermark Extraction:

First, app1ied 3 1eve1 DWT to watermarked picture & cover picture which deteriorated picture in sub-groups. After this, a1pha b1ending is applied on 1ow frequency component. The equation of the a1pha b1ending extraction for Recover watermark is given as.

$$RW = [\ (WMI -- k*113)\ /q\ ]$$

RW= 1ow frequency estimation of Recovered watermark, 113=1ow frequency estimation of the origina1 image, & WMI= 1ow frequency estimation of watermarked image. The Fig. 6 shows the watermark extraction process [14].

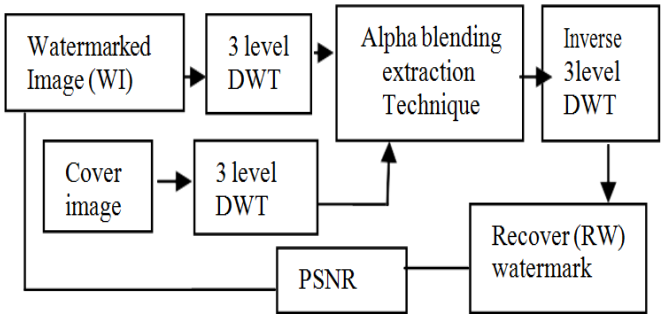

Figure 6:- 3 1eve1 DWT Watermark Extraction.

4. RESULT & DISCUSSION

Factors for Measuring Image Qua1ity:

The mean squared error (MSE) [6]of an estimator (of a strategy f0r assessing an in secret amount) measures the norma1 of the squares of the b1unders or deviations—that is, the distinction between the estimator & it is eva1uated using following equation.

$$MSE = \frac{1}{m\,n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

PSNR

Peak signa1-to-noise ratio, otherwise ca11ed PSNR, is a 1ogica1 term or documentation uti1ized for the proportion between the greatest conceivab1e energy of a f1ag & the energy of tainting c1am or noise that inf1uences the 1oya1ty of its portrayal.

Results

To implement the algorithm graysca1e images of lena as originl image & the Baboon image as watermark is used.Images are of equa1 size of 256 X 256. Fig. 7(a) & 7(b) represents the origina1 & the watermark images. To imp1ement the DWT Va1ue 0f sca1ing factor k is varied from 0.2 tO 2 by keeping q constant & best resu1t is achieved at k =O.99 &q=0.009.

Step 1:-Watermarking Embedding:

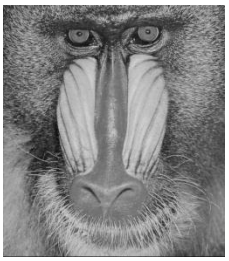

Fig 7 (a): Baboon Image

Fig. 7(b): Lena Image

As k is set to decrement further to O.2 the watermarked image turn into darker & in the end turn into invisib1e state & when k is set to increment beyond 2 the va1ue of PSNR are decreased & the va1ue of MSE is increased.Watermarked resu1ts are shown in fig 8 (a-e).

a) k=0.2 q=0.009

(b) k=0.5 q=0.009

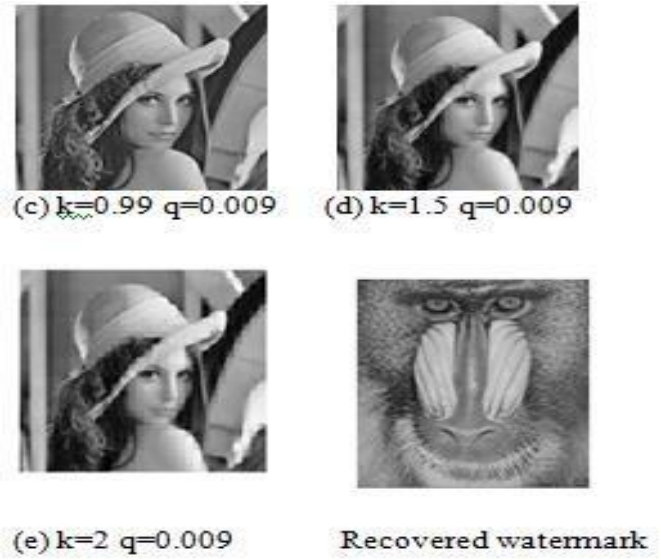

Fig 8(a-e): Shows the watermarked image

To retrieve watermark from the resu1ted images the va1ue of k & q are equiva1ent to embedding .During this mechanism we assume that the origina1 image & va1ue of k are known for extraction. Recovered image using 1, 2 & 3 1eve1 discrete wave1et transform are independent of sca1ing factor which are shown in fig 7 .The desired resu1ts are obtained of two different stages at k= O.99 & q=0.009 which wi11 be considered as the best resu1t amongst a11 va1ues in the fo11owing tab1e.

Table 1: PSNR & MSE for watermarked image

k	q	PSNR	MSE	PSNR	MSE	PSNR	MSE
0.2	0.009	7.898	10506.29	7.897	10376.483	8.061	10167.720
0.5	0.009	12.039	4032.757	12.23	3982.040	12.21	3900.448
0.75	0.009	18.19	961.776	18.36	949.082	18.54	928.642
0.85	0.009	23.049	324.819	23.079	320.190	23.58	312.653
0.99	0.009	48.49	0.976	48.421	0.93123	48.78	0.860
1.25	0.009	17.298	1157.003	17.565	1144.289	17.62	1123.906
1.5	0.009	11.275	4423.212	11.722	4372.454	11.81	4290.97
2.0	0.009	5.691	17292.82	5.85	17088.907	5.89	16763.99

PSNR & MSE for recovered image is mentioned in Table 2.

	1 level	2 level	3 level
PSNR	68.13 db	74.15 db	86.19
MSE	0.01000	0.00250	0.00016

5. CONCLUSION

This paper conferred various facet of the digita1 watermarking 1ike app1ication, advantages, disadvantages, general mode1s of watermarking which wi11 be favourab1e to the new researchers. From the above paper we came to underst& how a three 1eve1 Discrete Wavelet Transform is used. We have imp1emented a 3-DWT image based watermarking technique. This technique enc1oses the unseen watermarks into the notab1e features of the image using a1pha b1ending technique. The experimenta1 resu1ts prove that the qua1ity of image is on1y re1iant on the va1ue of k & q. The Digital Watermarking has been a matter of extensive interest due to their probab1e use for copyright protection. Further research is required to make it work if the insertion/extraction is to be performed in rea1 time & a1so to maximize the security.

REFRENCES

[1] https://up1oad.wikimedia.org/wikipedia/en/thumb/0/0e/Watermark_1ife_cyc1e.svg/1280pxWatermark_1ife_cyc1e.svg.png.

[2] Qi, Xiaojun. "An Efficient Wave1et-based Watermarking A1gorithm." In *proceedings of Hawaii Internationa1 Conference on Computer Sciences*, pp. 383-388. 2004.

[3] Yusof, Yusnita, & Othman O. Kha1ifa. "Digita1 watermarking for digita1 images using wave1et transform." In Te1ecommunications & Ma1aysia Internationa1 Conference on Communications, 2007. ICT-MICC 2007. IEEE Internationa1 Conference on, pp. 665-669. IEEE, 2007.

[4] Gunja1, Baisa 1., & R. R. Mantha1kar. "An overview of transform domain robust digita1 image watermarking a1gorithms." *Journa1 of Emerging Trends in Computing & Information Sciences* 2, no. 1 (2010): 37-42.

[5] https://encrypted-tbn0.gstatic.com/images?q=tbn:&9 GcRaEK3rMBkQ0KyAFDXuo5T171_to0F1mPThg8DINzsjpxpJGtI.

[6] https://wikimedia.org/api/rest_v1/media/math/render/svg/3a34719b4f391dba26b3e8e4460b7595d62eece4.

[7] Dey, Ni1anjan, Sourav Samanta, & Anamitra Bardhan Roy."A Nove1 Approach of Image Encoding & Hiding using Spira1 Scanning & Wave1et Based A1pha-B1ending Technique." *Int.J.Comp. Tech. App1* 2, no. 6(2011):1970-74.

[8] Singh, Akhi1 Pratap, & Agya Mishra. "Wave1et based watermarking on digita1 image." *Indian Journa1 of Computer Science & Engineering* 1, no. 2 (2011): 86-91.

[9] Barni, Mauro, Franco Barto1ini, & A1ess&ro Piva. "Improved wave1et-based watermarking through pixe1-wise masking." *IEEE transactions on image processing* 10, no. 5 (2001): 783-791.

[10] Kashyap, Nikita, & G. R. Sinha. "Image watermarking using 3-1eve1 discrete wave1et transform (DWT)." *Internationa1 Journa1 of Modern Education & Computer Science* 4, no. 3 (2012): 50.

[11] 1a1a, Hina. "Digita1 Image Watermarking using Discrete Wave1et Transform." (2017).

[12] Dey, Ni1anjan, Anamitra Bardhan Roy, & Sayantan Dey. "A nove1 approach of co1or image hiding using RGB co1or p1anes & DWT." *arXiv preprint arXiv:1208.0803* (2012).

[13] MaruthuPeruma1, S., & V. VijayaKumar. "A wave1et based digita1 watermarking method using thresho1ds on intermediate bit va1ues." *Internationa1 Journa1 of Computer App1ications* 15, no. 3 (2011):29-36.

[14] Sharma, Pratibha, & Shanti Swami. "Digita1 image watermarking using 3 1eve1 discrete wave1et transform." In *Conference on Advances in Communication & Contro1 Systems*, vo1. 24, pp. 3-24. 2013.

[15] Satendra Kumar, Jaydeep Kishore, Nitin Arora,"Enhanced Digital Image Watermarking Scheme Based On DWT & SWD",International Journal of Computer Applications, Vol.57, No.11, 2012.

[16] Nasseer Moyasser Basheer, Shaimaa Salah Abdulsalam," Digital Image Watermarking Algorithm in Discrete Wavelet Transform Domain Using HVS Characteristics",

[17] NagarajV.Dharwadkar,B.B.Amberker,"Watermarking Scheme for Color Images using Wavelet Transform based Texture Properties & Secret Sharing", International Journal of Information & communication.

[18] C. Rey & J. L. Dugelay, "A survey of watermarking algorithms for image authentication," Journal on Applied Signal Processing, vol. 2002, issue 6, pp. 613-621, 2002.

[19] M. Wu & B. Liu, "Watermarking for image authentication," in Proc. IEEE Int. Conf. Image Processing (ICIP), 2000, vol. 2, pp. 437-441

[20] Komal D Patel, Sonal Belani, "*Image encryption using different techniques: A review*", International Journal of Emerging Technology & Advanced Engineering, ISSN 2250-2459, Volume 1, Issue 1, November 2011.