A Review on Geometric Invariant Digital Image Watermarking Techniques

Amitesh Kumar
M.Tech CSE
School of Computing Science
and Engineering
VIT University

V. Santhi
Associate Professor
School of Computing Science
and Engineering
VIT University

ABSTRACT

In recent days the computer communication and the usage of multimedia data is enormous in the Internet, so protection of those data from malicious attacks and signal processing operations are very important. In specific, geometric attacks are considered as serious attacks which make watermarked work get distorted such that it is difficult to extract hidden information. In this paper the detailed study is made on the various geometric attacks invariant watermarking algorithms and also a comparative study report is present for geometric attacks invariant watermarking systems.

Keywords

Digital Watermarking, Geometrical Distortion, Transform domain watermarking

1. INTRODUCTION

With the rapid development of digital multimedia and the web technology, the application of multimedia (video, audio and image etc) has been widely spread. As the application increases, the issue on the security of the copyright has been receiving more and more attention recently. The concept of digital watermarking basically came at the time of trying to solve the problems related to the management of intellectual property of media [1].

The basic cryptographic system allows only valid key user to access the encrypted data. But once it is decrypted it is no longer secured. So a new system which provides security even after decryption of the data is digital watermarking system [2]. Digital watermarking is one of the effective technologies to protect the multimedia products by embedding a watermark into the target or source product. Digital watermarking is a visible or invisible identification code that is permanently embedded in to the cover data. This digital watermarking could be used to prove the reliability of products, track the pirates and authenticate the owner's right on the product [3]. In Fig.1 a typical watermarking system is shown, which includes watermark embedder for embedding the watermark in the cover data using a secret key and watermark detector for extracting the watermark using the same key. Here key is used to make the whole system more secure [4].The input of the watermark detector is watermarked image, security key and original cover data.

The watermark to be hidden is W, I is the cover image and K is the security key in watermarking system. The embedding function E (.) takes the watermark W, the cover image I, and security K, as the input parameters, and outputs the watermarked data I'. In Eq.1 the input parameters are given to the embedding function and it produces watermarked data as output. The input parameters are data to be marked called as cover data, watermark to be hidden and a key for hiding watermark in a secured way.

$$I' = E(I, W, k) \qquad (1)$$

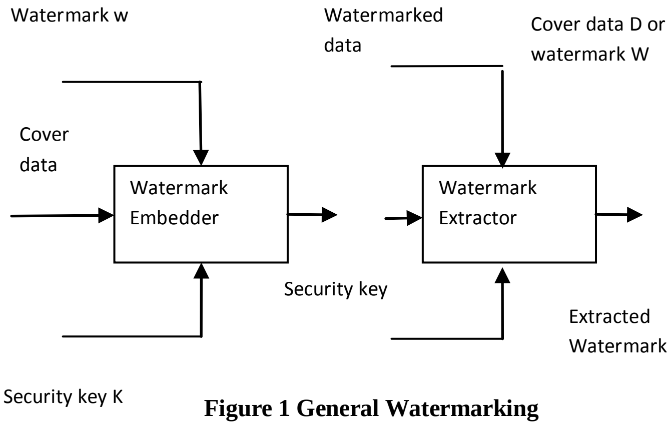

Figure 1 General Watermarking System

Theoretically the watermarking algorithm is consider as robust if it is embedded in such a way that the watermark can remain present even the watermarked data I' is passed though severe kind of distortions. The watermark detection procedure is presented in Eq. 2

$$W = D(I', k) \qquad (2)$$

The basic requirements of any watermarking system are as follows [5].

1. The watermark W' (extracted watermark after distortion) can be detected from I' with/without requiring explicit knowledge of I
2. I' should be very close to I in most of the possible cases
3. If I' is unchanged then detected watermark W' exactly matches W
4. In the robust watermarking, if cover image I' get modified, W' should still match W up to maximum extent to give authentication of the existence of the watermark.
5. In the fragile watermarking, if cover image I' get modified W' will also be totally changed from W even if minute change takes place in I'.

1.1 Classification of Digital Watermarking

Digital watermarking can be classified into different categories on the basis of host signal as follows

1. Digital Image Watermarking: In present scenario most of the research in digital watermarking is focused on image watermarking. There might be many reasons behind it such that as these days many images are available on the internet at free of cost without any copyright protection mechanisms [6].

2. Digital Video Watermarking: A video sequence consists of still images therefore all the watermarking methods applied on image could also be applied on video sequences [7].

3. Digital Audio Watermarking: In case of audio signals, “watermarking” can be defined as follows “Robust and inaudible transmission of additional data along with audio signals”. Audio watermarking is based on the Psycho-acoustic approach of perceptual audio coding techniques [8].

Another classification of watermarking system is based on the domain in which the watermark is embedded. If watermark is embedded by modifying the intensity value of the pixels then it is called spatial domain watermarking, if the frequency coefficients are changed then it is called transform domain watermarking system. Many transformation techniques are used for transforming image from spatial to frequency domain which includes Discrete Fourier Transform (DFT)[9] Discrete cosine Transform (DCT)[10], Discrete wavelet transform (DWT)[11] and Discrete Hadamard Transformation (DHT)[12].

Any watermarking system must possess the following properties [13].

Robustness

Robustness means the embedded image should be secure against different types of attacks. A good watermarking algorithm should be robust against signal processing operations, geometric attacks such as rotation, scaling and translation and lossy compression.

Imperceptibility

Invisibility is the most important concern of the watermarked image. The embedded watermark in the cover image should not be visible. The fidelity of the cover image should be maintained.

Capacity

The maximum amount of information that can be hidden without degrading the image quality is known as the capacity of the watermark. This amount depends upon the different kinds of application e.g. copyright protection, content authentication, fingerprints, broadcast monitoring etc.

2. GEOMETRIC DISTORTION

Geometrical distortion includes rotation, translation, scaling and shearing, projective transformation. Geometrical distortions are classified basically into two types [14] [15]

1. Global geometrical distortion
2. Local geometrical distortion

Global distortion affects all the pixels of the image in the similar manner while local distortion affects different portion of an image in different way.

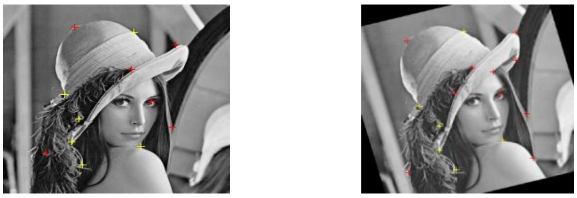

Figure 2(a) **Figure 2(b)**

Figure 2(a) and 2(b) Set of feature points of an unattacked image and atttacked image by united invasion respectively

The basic transformations which come under the geometrical distortion are as follows.

2.1 Rotation

Two dimensional rotations is applied to an image by repositioning it along a circular path in two dimensional XY plane. Let $f1(x,y)$ is achieved by rotating the image $f0(x,y)$ by a degree of θ in spatial domain

$$f1(x,y) = f0\big((xcos\theta + ysin\theta), (-xsin\theta + ycos\theta)\big) \quad (3)$$

2.2 Scaling

Scaling means changing the size of an image by either multiplying or by dividing the coordinate values (x,y) by scaling factors *a* and *b* to execute the transformed coordinates

$$\begin{cases} x' = x.a \\ y' = y.b \end{cases} \quad (4)$$

where a & b are the scaling factor along x-axis and y-axis respectively.

2.3 Translation

A shift is applied to an image by repositioning it along a straight line path from one coordinate location to other. A coordinate (x,y) is translated to a new position (x',y') by Eq. (5).

$$\begin{cases} x' = x + x_0 \\ y' = y + y_0 \end{cases} \quad (5)$$

3. INVARIANT TECHNIQUES TO GEOMETRIC DISTORTIONS

Geometric distortion affecting image and video data includes rotation, spatial scaling, and translation, skew or shear perspective transformation and change in the aspect ratio. Geometric distortion can be global; affecting all samples in same manner, or may vary locally. Although many different approaches have been investigated, robustness to geometric distortion remains one of the most difficult outstanding areas of watermarking research. Many works have been carried out to make the algorithm robust to geometric attacks. Some of the important techniques used are given below [16].

3.1 Exhaustive search

Exhaustive search is the simplest approach for watermark detection after the temporal and geometric distortion. It entails inverting a large number of possible distortion, and testing for a watermark after each one. As the number of possible distortion increases, the computational cost and false positive probability using this approach become unacceptable.

3.2 Synchronization or Registration

Synchronization or registration pattern can be embedded into cover image to simplify the search. This step prevents an increase in the false alarm rate and usually more computationally efficient as compare to exhaustive search.

3.3 Autocorrelation

The autocorrelation approach of a work typically has a large peak at zero and then decays rapidly at non–zero shift. This is even truer when examining the autocorrelation of a "white" or uniformly distributed signal. When a periodic, white synchronization pattern is embedded in a work, the resulting autocorrelation will contain a periodic train of peaks identifying the periodicity of the added pattern in the work. Thus in turn can be used to identify and invert any scaling applied to the work since embedding of the synchronization pattern.

3.4 Invariant watermark

Invariant watermark can be constructed in log-polar Fourier transform. These remain unchanged under certain geometric distortions, thereby eliminating the need to identify the specific distortions that have occurred.

3.5 Implicit synchronization

There is a class of blind detection watermarking technique in which the suspect work goes through a synchronization process prior to detection. However in place of synchronization pattern actual features of the work are used. This type of synchronization is called as implicit synchronization. Implicit synchronization requires that the salient features be reliably extracted during detection. Some distortion may affect the locations of the salient features relative to the work. When these distortions are applied after watermark embedding but before detection, the implicit synchronization can fail and watermark can go undetected [16].

4. APPLICATION OF DIGITAL WATERMARKING

The important applications of watermarking are listed below [6].

4.1 Copyright Protection

The idea behind copyright protection is to embed information about the copyright owner into the data or cover image to prevent the third parties from claiming to be the authenticated owner.

4.2 Copy and Usage control

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

4.3 Content Description

This watermark can contain some detailed information of the host image such as labeling & captioning. For this kind of application, the capacity of the watermark should be relatively large and there is no strict requirement for the robustness.

4.4 Content Authentication

Content authentication is able to authenticate the content, if any change to or tampering with the content should be detected. This can be achieved through the use of "fragile /semi-fragile watermark" which has low robustness to the modification of image. The semi-fragile watermark can also serve the purpose of quality measurement.

5. REVIEW ON GEOMETRIC INVARIANT WATERMARKING SYSTEMS

Review of watermarking techniques robust to geometric distortion is carried out and it is given below:

In [17] technique proposed with Human Visual System (HVS) characteristics and discrete wavelet transformation (DWT). By using a multi resolution data fusion approach, both image and watermark are transformed into wavelet domain to merge the watermark at the various resolution levels. This method is found to be robust as it embeds the watermark into more salient and strong components of the image. The performance of the algorithm is tested using host image as cover data and the binary image of size 32 as watermark. The algorithm is tested against attacks such as JPEG compression, additive noise and two dimensional linear mean filtering. The robustness of the technique is evaluated by normalized correlation coefficient of the extracted and original watermark. The algorithm is robust for the above said attacks. In [18] a digital image watermarking system is proposed using a Discrete Fourier Transformation (DFT) based on spread spectrum technique. Technique is robust against translation, rotation, and scaling and JPEG compression attacks. Though the method can be classified as a heuristic search, it maintains the search space relatively small, reducing the computational burden of the detection algorithm. To determine the performance, it tested several times against attacks such as collusion, domain filtering, noise addition, cropping etc.

In [19] a new technique is proposed based on the feature of image. The scheme is implemented in two phase, in 1st phase key is generated is using DCT technique and in 2nd phase watermark revelation takes place. In the secret key generation phase, the copyright owner extracts the image feature from DCT image in order to construct a bitmap *M* whose size is the same as that of the watermark W to be casted. Then apply the exclusive-or operation on the bitmap M and the watermark W to generate in secret key K. In 2nd phase watermark revelation can be divided into three steps. In the first step apply 4x4 DCT on the protected image to obtain a transformed image. In 2nd step use the secret seed $K_{s,}$ that is kept by the copyright owner and in final step reveal the watermark W' by applying the exclusive-or operation on the bitmap and the secret key K_s. DC coefficient are used to preserve the features of an image blocks.

In [20] a new watermarking approach is proposed in the form of public watermarking technique which is robust to geometrical attacks. This algorithm uses a normalization technique with respect to affine transformation of the image which is based on the moments of the image and discrete cosine-code division multiple access (DC-CDMA).In [21] a new watermarking technique for data hiding in media signal operating in the frequency domain using content based image segmentation is proposed. It uses the feature extraction techniques and Voronoi diagram. Voronoi diagram is used to define a group of segment in the host image based on the feature points to be watermarked. The segmentation induced by this model is called the Voronoi diagram of the set of the feature points. In [22] an algorithm is proposed to embed watermark log polar continuous Fourier Transform (FT). The image has been tested for geometrical attacks as well as JPEG coding also. In [23] two watermarking approaches are presented. First technique is multibit public watermarking scheme which is based on image normalization technique, aimed to be robust to general affine geometric attacks and second technique is based on a watermark resynchronization aimed to alleviate the effect of random bending attacks. In second scheme, a deformable mesh is used to correct the distortion caused by the attack, after the watermark is extracted from corrected image. The first watermarking system is suitable for public watermarking in which original image not necessary but the second technique is suitable for private watermarking in which original image is necessary for the detection.

In [24] a new watermarking technique which is based on the three-dimension (3D) mesh modeling which can be used for a number of different purposes is proposed. Before embedding the watermark, as a pre-process the model is transformed into the invariant space. A watermark sequence is embedded in the host with the modifying lengths between the vertices and the centered of the models in the DCT domain based on quantization technique to get the blind watermarking extraction. In [25] a new approach of watermarking algorithm is presented which is based on the feature point and Integer Discrete Wavelet Transform (IDWT) against the geometrical rotation and scaling. Here watermark embedded in such a way that it partially changes the arithmetical compliment of deep low frequency wavelet coefficient according to the watermark characteristics.

In [26] a robust watermarking approach based upon bi-dimensional empirical mode decomposition (BEMD) against geometric distortion is proposed. This method uses the orthogonal properties of bi-dimensional empirical mode decomposition (BEMD) to achieve the piece based orthogonal change in the image. This method allows study of non-linear and non –stationary data. It decomposes a given signal into many frequency components, called intrinsic mode function (IMF). All these decomposed parts of data or image having different frequency. Watermark is embedded into the intermediary frequency IMF. Middle frequency is adoptively weighted on the basis of image visual system and orthogonal transform. Experimentally it clears that this method can show the watermark when the image is half cut and having excellent robustness against image shearing. In [27] a new watermarking algorithm to confront the geometric transformation based on the feature points is proposed. Feature point is selected using the Robert operator and watermark is embedded in these regions. The algorithm is tested against normal image processing; Photoshop is used to extract the watermarking after JPEG compression with different quality factor. As the value of quality factor value goes down watermark image gets more distorted. For these quality factor Q, NC (Normalized Correlation coefficient) value is inversely proportional it's clear by experiment.

As per the survey, to design a geometric invariant watermarking system watermark embedding need to be carried out in transform domain. Watermark embedding could be carried out in two ways; one way is to extract the feature points before embedding, the other way is transforming the host image into feature invariant domain. To convert image into feature invariant domain normalization and log polar transformation techniques are used. To extract watermark from the distorted host data, synchronization and autocorrelation approaches are used.

In order to quantitatively analyze the invisibility and robustness of the algorithm, two parameters are used. First one is peak signal to noise ratio (psnr in dB), which is used to measure the invisibility of the watermark. The second one is correlation coefficient (NC) which is used to measure the correlation between the original and the recovered watermark.

To evaluate the performance of watermarking scheme, experiments have been conducted on various standard test images by introducing different kinds of attacks. The experiments on Lena Image of size 512X512 with single or united attack in different degree of rotation and different proportion of scaling have been listed in the Table 1 and Table 2. The estimations on single attack of rotation or scaling are showed in the Table 1. If the rotation angle is increased the amount of distortion is also increased which in turn changes the correction parameter. If the amount of distortion is less, then the correction parameter is also less otherwise the amount of correction required is almost equal to the amount of distortions introduced. In Table 2, the effect of both scaling and rotation attacks are shown. These attacks are implemented simultaneously and it is known as united attacks. As the values of rotation angle and scaling parameter changes, then the correction value in rotation angle and scaling parameter also changes.

Table1. Estimation of Single Attack of Rotation or Scale

	Rotation Angle		Scaling parameter	
	Distortion	Correction	Distortion	Correction
1	1	0.4975	0.5	0.4942
2	5	4.8871	0.9	0.8979
3	10	10.0494	1	1
4	20	19.8314	1.1	1.0992
5	45	45.0781	1.29	1.2997
6	60	60.0275	1.49	1.4899
7	80	80.2282	1.71	1.7120

Table 2.Estimation on United Attack of Rotation and Scale

	Distortion		Correction	
	Rotating Angle	Scaling Parameter	Rotating Angle	Scaling Parameter
1	4	1.5	3.8732	1.4971
2	10	0.9	10.1262	0.8987
3	15	1.21	15.1132	1.2135
4	60	0.6	59.6261	0.5860
5	80	0.81	80.1110	0.8142

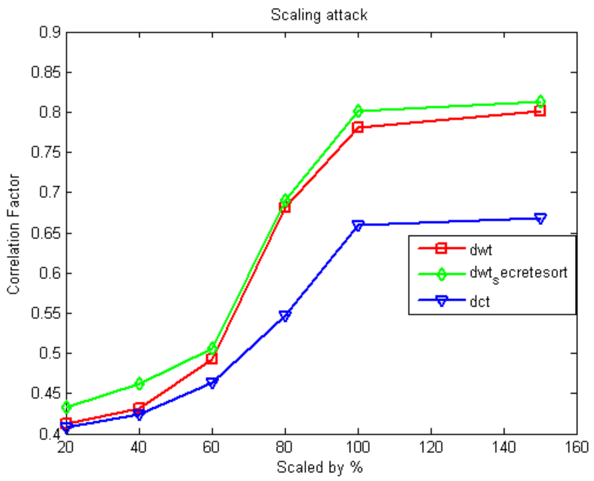

Figure 3 Correlation factor of different watermark method based on scaling attacks

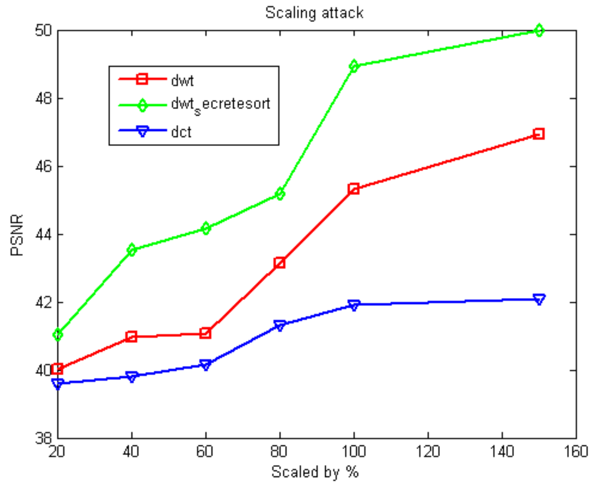

Figure 4 PSNR of different watermarking methods based on scaling attack

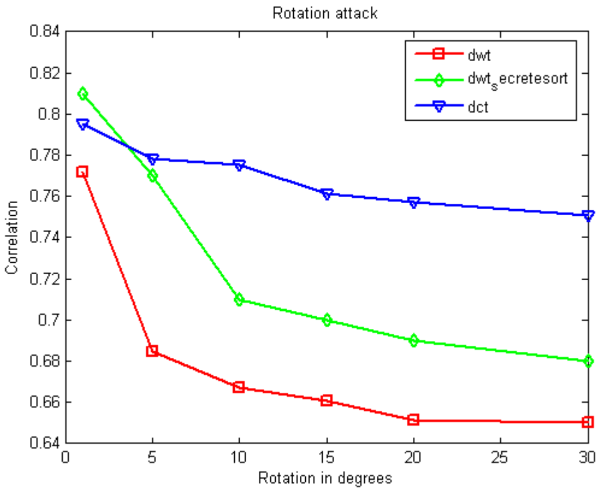

Figure 5 PSNR of different watermarking methods based on rotation attack

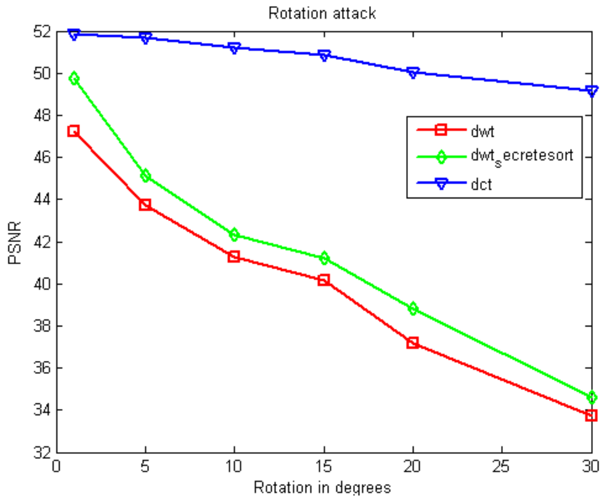

Figure 6 Correlation factors of different watermarking methods based on rotation attack

Scaling: Figure 3 and 4 shows the result of extracting watermarks from scaled watermark images. When watermark image is scaled to 20% and 40% DCT and DWT techniques failed to extract watermark [28].

Rotation: Figure 5 and Figure 6 show the result of extracted watermark result of extracted watermarks from rotated watermarked image. DCT method is having better PSNR(Peak Signal to Noise Ratio) and correlation factor values for different angles of rotation compared to DWT .

6. CONCLUSION

In this paper, detailed study is made on several RST invariant techniques. In many of the papers spread spectrum based schemes are used to make watermarking system more robust to RST attacks. Similarly, RST invariant features extraction schemes are used in few papers. Many of the work are carried out in RST invariant domain using normalization technique.

As per the survey to design a geometric invariant system watermark embedding need to be carried out in transform domain. To convert image into feature invariant domain, normalization and log polar transformation techniques are used. To extract watermark from the distorted host data, synchronization and autocorrelation approaches are used. Thus though each technique is having its own advantages and disadvantages they are more robust to RST attacks.

7. REFERENCES

[1] H Kwon,Y S Kim, R H Park "A Variable Block-Size DCT Based Watermarking Method" Volume 45,Issue : 4; pp: 1221-1229 IEEE 1999.

[2] B J Falkowski, L-S Lim "Image Watermarking Using Hadamard transforms EL Vol. 36 No 3, pp:211-213 IEEE 2000.

[3] J. Dittmann, P.Wohlmacher, K. Nahrstedt "Using Cryptographic and Watermarking Algorithms" Multimedia and Security Volume:8, Issue:4 pp:54-65 IEEE 2001.

[4] Y Wang, J F. Doherty, R E.V Dyck " A Wavelet-Based Watermarking Algorithm for Ownership Verification of Digital Image" IEEE Transaction on Image Processing , Vol.11, No 2, pp:77-88 Feb 2002

[5] A Shan, E Salari “Real-Time Digital Video Watermarking” TUAM 2.1 ICCE pp:12-13 IEEE 2002

[6] P Bas, J-M Chassery, B Macq “Geometrically Invariant Watermarking Using Feature Points” IEEE Transaction on Image Processing, Vol 11, No 9,pp:1014:1028 Sep 2002

[7] D.Bogumil, “Reversing global and local geometric distortions in image watermarking”, in proc information hiding 2004, pp25-37.

[8] A Lang, J Dittmann, R Spring, C Vielhauer “Audio Watermark Attacks: From Signal to Profile Attacks” MM- SEC’ 05, August, 2005, ACM, NY, USA.

[9] Ping Dong, Jovan G. Brankov, Nikolas P.Galatsanos,Yongyi Yang & Frank Davoine “ Digital Watermarking Robust to Geometric Distortions ” IEEE Transaction on Image Processing, Vol.14, NO. 12,DECEMBER 2005

[10] Liu Liang , Sun Qi “ Robust image Watermarking against geometrical attack” pp: 1-3 IEEE ICWMNN 2006 Proceedings

[11] Dan Wang, Peizhong Lu “A Novel Geometrical Robust Image Data Hiding Scheme” Workshop on Image Analysis for Multimedia Interactive Services (WIAMIS 2007) pp: 59-59

[12] J. A M Polanco, A. C P Garcia, R R Colin,C F Uribe “Digital Watermarking Based on Image Centroid resistant to rotation and scalling” International Conference on Electronics,Communication and Computers (CONIELECOMP’07) ,pp: 33-33

[13] Dong Zheng ,Y Liu,J Zhao, A E Sadik “A survey of RST Invarient Image Watermarking Algorithm” , ACM Computing Surveys , Vol 39, No-2, Article 5, June 2007.

[14] Xiu-mei Wen, Wei Zhao, Fan-xing Meng “Research of a Digital Image Watermarking Algorithm Resisting Geometrical Attacks in Fourier Domain” pp: 265-268, IEEE 2009

[15] Z Xiaoli, Lv Xin “ A Novel Watermarking Algorithm Resist to Geometrical Attack” IEEE International Conference on Electric Commerce and Business Intelligence 2009, pp:503-506

[16] I J Cox,M L Miller,J A Bloob “ Digital Watermarking” Morgan Kaufmann Publishers, *Second Edition*

[17] D Kundur,D Hatzinakos “ A Robust Digital Image Watermarking Method using Wavelet-Based Fusion” page(s) : 544-547 vol.1, IEEE 1997

[18] V Licks, R.Hordan “ On Digital Image Watermarking Robust to Geometric Transformations” pp: 690 - 693 vol.3 IEEE 2000

[19] C-C Chang,J-C Yeh,J-Y Hsiao “ A Method for Protecting Digital Image from Being Copied Illegally” pp:373-379 IEEE 2001

[20] P Dong, N P Galatsanos “Affine Transformation Resistant Watermarking Based on Image Normalization” pp: 489 - 492 vol.3 IEEE June-2002

[21] M.A.Suhail, M.S.Obaidat “ A Watermarking Technique For Geometric Manipulation Attack” Publication Year: 2005, pp: 1 - 5 IEEE .

[22] M Ossonce, C Delpha, P Duhamel “ Rotation and Scale Insensitive Image Watermarking” pp: 2611 - 2614 Vol. 4 International Conference on Image Processing(ICIP) 2004

[23] Ping Dong, Jovan G. Brankov, Nikolas P.Galatsanos,Yongyi Yang & Frank Davoine “ Digital Watermarking Robust to Geometric Distortions ” IEEE Transaction on Image Processing, Vol.14, NO. 12, pp: 2140 - 2150 DECEMBER 2005

[24] W Liu, S H Sun “ Rotation ,Scaling and Translation Invarient Blind Digital Watermarking for 3D Mesh Models” International Conference on Innovative Computing,Information and Control(ICICIC’06) pp: 463 – 466, IEEE 2006

[25] Z Xiaoli, Lv Xin “ A Novel Watermarking Algorithm Resist to Geometrical Attack” IEEE International Conference on Electric Commerce and Business Intelligence 2009, pp: 503 - 506

[26] D Menghui, Z Jingo “ Robust Image Watermarking Algorithm against Geometric Attack Based on BEMD” International Conference on Computer and Communication security IEEE 2009, pp: 36 - 39

[27] T Wenliang “ A Feature –Based Digital Image Watermarking Algorithms Resisting to Geometrical Attack” International Sysposium on Electronic Commerce and Security IEEE 2009, pp: 174 – 178.

[28] K.Ramani, E.V. Prasad , S.Varadarajan , A. Subramanyam “ A Robust Watermarking Scheme for Information Hiding” ADCOM , IEEE 2008, pp: 58 - 64

Prof..V.Santhi is currently working as Associate professor in VIT University, Vellore , India. She is having more than 15 years of teaching and more than 3 years of Industry experience. She has pursued her B.E degree in Computer Science and Engineering from Bharathidasan University, Trichy and M.Tech degree in Computer Science and Engineering from Pondicherry University, Pondicherry. She is currently doing PhD in VIT University. She is a member of IACSIT, IEEE and CSI. Her area of research includes Image Processing, Digital Signal Processing, Digital Watermarking and Data Compression. She has published many papers in international conferences and Journals

Amitesh kumar is currently pursuing M.Tech. Computer Science and Engineering in VIT University, Vellore, India. He has completed his Bachelor of Engineering from Institute of Engineering and Technology, Agra University, Agra, India. He is a member of IEEE and CSI. His area of interest includes Image Processing, Digital Watermarking and Networking.