Image Watermarking Using Geometric Moments

L.Kalyan kumar¹, KSrinivas Reddy², Dr.Syed Musthak Ahmed³

Department of Electronics and communication Engineering, M-Tech Embedded systems, S.R. Engineering college,

Andhra Pradesh, Warangal, INDIA.

Abstract: Image watermarking is a method that embeds a watermark in the digital image by making small changes in the host data. The embedded watermark must be perceptually invisible and it must be difficult to change or remove it against the intentional or unintentional attacks such as compression, linear and non linear filtering and geometric transformations.

In watermarking applications, the robustness of the watermark to the common signal processing and geometric attacks is essential to the system. The paper presented a method, based on scale and rotation information estimated from the edges of the image. Fleet proposed an approach in which the watermark is composed of the sum of sinusoids that appear as peaks in the frequency domain which can be used to determine the geometric distortion. A different approach was presented in which watermark is inserted in rotationally, scale and translation invariant parameters based on Fourier mellintransform. However, this method is based on discrete Fourier transform of the image which is highly sensitive to dropping and it cannot survive aspect ratio and rotationally attacks.

In order to survive geometric attacks, it is like to develop a watermarking method using Geometric moments. Geometric moments have been intensively used in the literature for image

recognition, template matching etc. This proposed a robust scheme test the method using the geometrically distorted software generated using stir mark and mat lab software's.

In order to overcome some of the disadvantage of existing methods and to obtain an invariant watermark an image watermarking technique using geometric moments invariable is proposed in this watermarking section and detection algorithm is presented in order to verify the proposed approach, simulation results are carried out. It also verified the invariance property of moment's invariant by considerly standard images. The proposed approach in robust, invariant, computationally efficient and no over head needed to transmit to the decoder side. The proposed approaches have proven to be highly robust to geometric manipulations and image compression.

I. INTRODUCTION

An image may be defined as a two-dimensional function, f(x, y), where x and y are spatial (plane) coordinates, and the amplitude of f at any pair of coordinates (x, y) is called the intensity or gray level of the image at that point. When x, y, and the amplitude values of f are all finite, discrete quantities, we call the image a digital image[1][2]. The field of digital image processing refers to processing digital images by means of a digital computer. A digital image is composed of a finite number of elements, each of which has a particular location and value. These elements are referred to as picture elements, image elements, pels, and pixels. Pixel is the term most widely used to denote the elements of a digital image. Interest in digital image processing methods stems from two principal application areas



Image Procession

A. Applications Of Digital Image Processing

Some of the areas where Digital Image Processing is widely used are

- Automatic character recognition
- Image watermarking
- Industrial machine vision for product assembly and inspection
- Military recognizance
- Automatic processing of fingerprints
- ➤ X-ray Imaging
- ➢ Satellite Imaging
- ➢ Radar Engineering etc.

II. WATERMARKING BASIC CONCEPTS

The recent growth of networked multimedia systems has caused problems relative to the protection of intellectual property rights. This is particularly true for image and video data. The types of protection systems involve the use of both encryption and authentication techniques. In this paper we describe a form of authentication known become available in digital form. It may be that the ease with which perfect copies can be made will lead to largescale unauthorized copying which will undermine the music, film, book and software publishing industries.

A. Features Of Invisible Watermarks

From the applications mentioned in chapter one, one can divide watermarks in two distinct types: robust, for the first five applications and fragile for the last three. The fragile watermarks are meant to disappear if the image (or other data used) is corrupted..

- Perceptual Transparency:
- Robustness:
- Capacity:
- Payload of watermark:.
- Security:
- Specificity:

III. GEOMETRIC MOMENTS

The Geometric moments of order (p, q) of an image function f(x, y) are defined [1] as

$$M_{pq} = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} x^p y^q f(x, y) dx dy \qquad (1)$$

Where $p, q = 0, 1, 2, \dots, \infty$

The above definition has the form of projection of an image function f(x, y) on to the continuous

monomials $x^p y^q$. To keep the dynamic range of M_{pq} consistent for different size images, the N x M image plane is first mapped onto a square defined by $x \in [-1,+1], y \in [-1,+1]$. This changes the definition of M_{pq} to

$$M_{pq} = \int_{-1-1}^{1} \int_{-1-1}^{1} x^{p} y^{q} f(x, y) dx dy \qquad (2)$$

The discrete form representation of the above expression is given by

$$M_{pq} = \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} x_i^p y_j^q f(x_i, y_j) \Delta x \Delta y$$
(3)

Where (x_i, y_j) is the centre of (i, j) pixel and $\Delta x = x_i - x_{i-1}$, $\Delta y = y_j - y_{j-1}$ are the sampling intervals in the 'x' and 'y' directions respectively. N x M corresponds to the size of the image.

The Geometric central moments [1] are defined as

$$\mu_{pq} = \int_{-\infty-\infty}^{\infty} \int_{-\infty-\infty}^{\infty} (x - \bar{x})^p (y - \bar{y})^q f(x, y) dx dy \qquad (4)$$

Where
$$\bar{x} = \frac{M_{10}}{M_{00}}$$
 and $\bar{y} = \frac{M_{01}}{M_{00}}$ (5)

For a digital image, the Geometric central moments can be expressed as

$$\mu_{pq} = \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} (x_i - \bar{x})^p (y_j - \bar{y})^q f(x_i, y_j) \Delta x \Delta y \quad (6)$$

The normalized central moments are defined as

$$\eta_{pq} = \frac{\mu_{pq}}{\mu_{00}^{\gamma}} \quad \text{Where} \quad \gamma = \frac{p+q}{2} + 1 \quad \text{for}$$
$$p+q = 2, 3, \dots$$

Geometric moments are the simplest among all other moments. These moments can easily be computed. Hu [1] derived moment invariants using Geometric moments which are invariant to image rotation, translation and scale.

A. Moment Invariants

Define the geometric moments M_{pq} of a grayscale image f(x, y) as

$$M_{pq} = \iint x^p y^q f(x, y) dx dy (1)$$

$$\mu_{pq} = \iint (x - \bar{x})^{p} (y - \bar{y})^{q} f(x, y) dx dy$$
(2)

where
$$\bar{x} = \frac{M_{10}}{M_{00}}$$
 and $\bar{y} = \frac{M_{01}}{M_{00}}$ are (3)

the centroids of the image. Define the normalized central moments $\eta_{p,q}$

$$\eta_{pq} = \frac{\mu_{pq}}{\mu_{00}^{\gamma}}$$
 Where $\gamma = \frac{p+q}{2} + 1$ for
 $p+q = 2, 3,$ (4)

. .

B. Invariance To Orthogonal Transformation

The following seven functions are invariant to orthogonal transformation (15) $\phi_1 = \eta_{2,0} + \eta_{0,2}$

$$\begin{split} \phi_{2} &= (\eta_{2,0} \ \eta_{0,2})^{2} + 4\eta_{1,1}^{2} \\ \phi_{3} &= (\eta_{2,0} \ \eta_{0,2})^{2} + (\eta_{0,3} \ 3\eta_{2,1})^{2} \\ \phi_{4} &= (\eta_{3,0} + \eta_{1,2})^{2} + (\eta_{0,3} + \eta_{2,1})^{2} \\ \phi_{5} &= (\eta_{3,0} \ -3\eta_{1,2})(\eta_{3,0} + \eta_{1,2})_{\times} \left[(\eta_{3,0} + \eta_{1,2})^{2} - 3(\eta_{2,1} + \eta_{0,3})^{2} \right] \\ &+ (\eta_{0,3} - 3\eta_{2,1})(\eta_{0,3} + \eta_{2,1})_{\times} \left[(\eta_{0,3} + \eta_{2,1})^{2} \right] \end{split}$$

$$-3(\eta_{1,2}+\eta_{3,0})^2$$

Similarly for \emptyset_6 and \emptyset_7 It should be noted that ϕ_7 is invariant to reflection in the ab- solute value only. It is worth mentioning that scaling, rotation, and flipping are all considered within the class of orthogonal transformation. In order to test the invariance of the ϕ 's to the various attacks, we performed the Stir Mark attacks on Barbara image. Table II shows the absolute log values of the invariants $\emptyset^* = |\log_{10} \emptyset|$ for the original image, the underlined values, and after attacks. ϕ^* were used instead of ϕ in the computations in

 φ were used instead of φ in the computations in order to reduce the dynamic range for illustration purposes. Examining Table II reveals the robustness of the invariants to almost all Starmark attacks. However, they are less robust to over cropping, aspect ratio change, and histogram modification.

IV. WATERMARK INSERTION SCHEME

Consider watermarking an image using the $\phi's$ invariants. It should be noted that the same approach can be also used with the $\psi's$ as well. Let $\phi_1^* = (\phi_1^* \ \phi_2^* \dots \phi_7^*)^T$ be the invariants of an image I, then the received image is Ir declared authentic if

$$N - \epsilon \leq f\left(\frac{\emptyset^*}{I_r}\right) \leq N + \epsilon$$
 (5)

Where f (a/b) means f(a) given b. The constant N is a nominal value, and (*esp.) is small tolerance determined experimentally as explained below. It should be noted that (5) implies that the original image I should be modified in order to achieve such a constraint. This is due to the fact that originally $f(\frac{\phi^*}{l})$ does not have to be equal to N. this can be achieved by finding a perturbation image ΔI such that

$$\Delta I = \beta \pi(I)$$
(6)
Added to the original image I such that

$$I^{\sim} = I + \Delta I \tag{7}$$

Satisfies (5), where II is a mapping function and β is a weighting factor. Fig.4. shows the encoder in which the mapping process is clear. It should be noted that β controlled by feedback in order to ensure that $N = f(\phi^*/I^{\sim})$.

A. Watermark Detection Scheme

In order to determine if the received image I_r^* is watermarked or not, the decoder simply checks the validity of (5). In particular, let the error E be

$$E = \left| f\left(\frac{\phi^*}{l_r^*}\right) - N \right| \tag{8}$$

The received image is declared authentic if $E \leq \in$; otherwise it is declared unauthentic. Two observations need to be clarified at this point. It is clear from the decoding process that the decoder does not need the original image in the decoding process, which is advantageous. The decoder only needs to know the constant N and the margin of error beforehand. Secondly, since the decoder checks the validity of (5) for the received image, then this water- marking scheme answers a yes/no question, authentic or not, i.e., this watermarking scheme is of 1-bit capacity. Determination of N and \in :

Since $N = f\left(\frac{\phi^*}{l_r^*}\right)$. Then N can be chosen to be any value near $f\left(\frac{\phi^*}{l_r^*}\right)$ by varying β As illustrated in fig.4. However, varying N affects the contrast of the watermarked image as explained in the next subsection.

Design of the Mapping Π :

It is clear from (7) that $\Pi(I)$ serve as noise added to the original image with β in order to modify the invariants. Hence, the weighting factor β should be as small as possible and at the same time $f(\frac{\phi^*}{l})$ should be within \in from N. consider fig.3 in which two model function Π_1 and Π_2 are used to map I into ΔI . As seen from the figure, Π_1 has faster variation rate with β than Π_2 . Thus by using the mapping Π_1 , small perturbation in β leads to large variation in $f(\frac{\phi^*}{l})$.

Design of $f(\emptyset^*)$ and $f(\Psi^*)$:

The function $f(\emptyset^*)$ can be chosen to be any function of invariants, i.e., linear or nonlinear. Also, for security purpose, secret key should be involved in the function design. For illustration purpose is expressed as a weighed average of the \emptyset^* s as follows

$$f(\emptyset^*) = \Xi(\omega_1 \emptyset_1^* + \omega_2 \emptyset_2^* + \dots + \omega_7 \emptyset_7^*)$$
(9)
$$f(\Psi^*) = \Xi(v_1 \Psi_1^* + v_2 \Psi_2^* + v_3 \Psi_3^* + v_4 \Psi_4^*$$
(10)

or from the Ψ^* 'Where Ξ is a secrete key operator which provides the required security for the watermark design. For simplicity and for illustration purpose in this paper, Ξ was chosen to be the transparent operator, i.e., $\Xi(x)=x$. The weights ω 's and ν 's should be chosen to minimize the perturbation in *f* if the invariants \emptyset^* 's and Ψ^* 's have been changed, due to an attack, to make the watermark move robust. One heuristic is to let the v's and the ω 's equal to the inverse of the variance of the values in each column in table I and II, respectively. This would minimize the perturbation in *f* for these attacks. However, doing so would yield a higher value of β since the variation in the function f would be minimized. This will result in less transparent watermark. One good choice is to the mean of the invariant, i.e., let *f* be

$$f(\emptyset^*) = 1/7 \sum_{i=1}^{i=7} \emptyset_i^* \tag{9}$$

$$f(\Psi^*) = 1/4 \sum_{i=1}^{i=4} \Psi_i^*$$
(10)

V. SIMULATION RESULT

In order to test the moment invariants, we have considered two images namely cameraman and tire each of size 256×256 . These images are subjected to reduction in scale by 0.9 and rotated by 10° . The original images are shown in fig: 5.1. The five moments invariant are computed and are listed in tables 5.1 and 5.2. From the results, it is observed that the computed invariant are same even the image is scaled and rotated. There is slight (neglible) variation in invariant values because of integral replaced by summation in the definition of moments. Hence, these invariants are used in this project work to obtain invariant image watermarking

Table.1.Geometric moment invariant computed for	
cameraman image	

Sl.N O	Invarian t Image	Orignal Image	Reduced To 0.9	Rotated By 10 ⁰
1	Ø ₁	-16.1992	-15.99	-16.49
2	Ø ₂	-37.85	-37.45	-38.44
3	Ø ₃	-52.95	-52.34	-53.84
4	Ø ₄	-52.47	-51.86	-53.36
5	Ø ₅	- 1.05e +002+3.14e	-1.09e +002+3.14	-1.06e +002+3.1
		+000i	+000i	4e +000i

Table.2.Geometric moment invariant computed for tire image

Sl.N O	Invariant Image	Orignal Image	Reduced To 0.9	Rotated By 10 ⁰
1	Ø ₁	-15.447	-15.23	-15.75
2	Ø ₂	-36.32	-35.9	-37.11
3	Ø ₃	-48.29	-47.68	-49.21
4	Ø ₄	-50.4	-49.82	-51.38
5	Ø ₅	-101.53	-100.27	-1.051e +002+ 3.14e+0 00i



(a)



(b)

5.1 Images used for computing invariants (a) Cameraman image (b) Tire image

VI. CONCLUSIONS

Watermarking is still in its infancy but has benefited tremendously from work on human Perception. We have presented a basic introduction to digital watermarking of image. Watermarking embeds ownership information directly into the document, and it is proposed as a "last line of defense" against unauthorized distribution of digital media. Desirable properties of watermarks include imperceptibility, robustness, and security.

VII. FUTURE SCOPE

In this project the channel noise was neglected. This will cause major problem because the receiver cannot retrieve the information correctly. Future work can be done keeping this into consideration. The further scope for this would be to best the approach when the images are corrupted by noise and chopping .In the approach there is slight contrast variation between the original image and watermark image. Improving the contrast differences between the original image and watermarked image. Improving the contract difference between the original and watermark image and improving the robustness to different geometric attacks robustness to different geometric attacks are possible direction for further work.

REFERENCES

- F. Petitcolas, R. Anderson, and M. Kuhn, "Attacks on copyright marking systems,"in *Proc. 2nd Workshop on Information Hiding*, Portland, OR, Apr. 1998, pp. 218–238.
- M. Alghoniemy and A. H. Tewfik, "Geometric distortion correction in image watermarking," in *Proc. SPIE Security and Watermarking of Mul- timedia Contents II*, vol. 3971, San Jose, CA, Jan. 2000, pp. 82– 89.
- 3) "Progressive quantized projection approach to data hiding," *IEEE Trans. Image Processing*, to be published.
- 4) M. Kutter, "Watermarking resisting to translation, rotation and scaling,"in *Proc. SPIE Int. Symp. Voice*,

Video and Data Communication, vol.3528, Boston, MA, Nov. 1998, pp. 423–431.

- D. Fleet and D. Heger, "Embedding invisible information in color images," in *Proc. Int. Conf. Image Processing*, vol. 1, CA, 1997, pp.532–535.
- M. Alghoniemy and A. H. Tewfik, "Progressive quantized projection watermarking scheme," in *Proc. 7th ACM Int. Multimedia Conf.*, Orlando, FL, Nov. 1999, pp. 295–298.
- J. O'Ruanaidh and T. Pun, "Rotation, scale and translation invariant dig- ital image watermarking," in *Proc. IEEE Int. Conf. Image Processing*, vol. I, 1997, pp. 536–539.
- 8) F. A. P. Petitcolas and M. G. Kuhn.. [Online] Available: <u>http://www.cl.</u> cam.ac.uk/fapp2/watermarking/stirmark/
- Y.Abu-Mostafa and D. Psaltis, "Recognitive aspects of moment in- variants," *IEEE Trans. Pattern Anal. Machine Intell.*, vol. PAMI-6, pp. 698–706, Nov. 1984.
- 10) Rafael C.Gonzalez, Richard E.Woods,Digital Image Processing, second edition, Pearson Education, 2002
- 11) Anil K.Jain, Fundamentals of Digital Image Processing, prentice-Hall
- 12) R.B. Wolfgang, C.I. Podilchuk and E.J. Delp, Perceptual Watermarks for DigitalImages and Video, *Proceedings* of the IEEE, Vol. 87, No. 7, July 1999, pp.1108-1126.

AUTHORS PROFILE



Mr.L.Kalyankumar received his M.tech degree from SR.Engineering college.warangal. J.N.T.U.In 2011.he had got ISTE Certificate on the arm controller and its applications .Presently he is working in the M.B.E.S.College of Engineering Ambajogai.

Mr.K.srinivasa reddy received his M.tech degree in J.N.T.U. He is working as Assoc. Prof in SR engineering college. He is member MISTE. Society. He had various Publication in national and international Journals/conferances.

Dr.syed Musthak Ahmed,completed his BE (Electronics) from Bangalore University,ME (Eletronics),UVCE Bangalore university,and Ph.D (ECE),Vinayaka mission University Salem.He had 25 years of teaching experiences working in reputed engineering college and presently working as professor and HOD (ECE),SR engineering college,Warangal. He is member of various professional societies like SMIEEE, FIETE,MISS ,MISTE ,MIAENG,MIAMT,He has various publication in National and International Journals/conferances