Fast Legendre Moments in Securing Digital Image

K. Alice Suresh, S. Thirunavukkarasu, P. Kavitha

Abstract: ***Moments are set of values used to describe the information contained in the image. In this paper the content of the image is represented with the help of fast legendre moments. Legendre moments has the advantage that these moments are calculated exactly without any loss in information while other moments like geometric moments, zernike moments etc suffer from approximation errors and geometric error when applied to digital images. Legendre moments are also more suitable for image reconstruction. Experimental results show that the proposed system is very efficient in computing moments at much faster time than the Zernike moments since fast legendre moments calculates the moments as two ID function rather as a 2D function of a digital image and the results of reconstruction in case of tampering is also shown.***

Keywords- Legendre moments, Zernike moments, Image forgery, Image reconstruction, Image representation, Image Security.

I. INTRODUCTION

Digital images are used in a wide range of applications for the past two decades and as a result of that many image editing applications challenges the security and integrity of images. There are many ways a hash can be generated by extracting local and global features [4],fixed point theory[7], watermarking methods [3][8], NMF[9][12], using fourier mellin transformation[12],DFT coefficients, radon transform co efficient as hash code [15],image histogram [13],DWT coefficients [3],[21] and much more. In recent work combining two or more hashing techniques to generate the hash code is also most common to make advantage of different hashing techniques [20]. The key aspects for a hash method are that it must be robust, compact and perceptive to forgery. In all the methods of available hash generation, self recovery in case of tampering is not or only partial addressed, because the information available for reconstruction is not completely described in hash. In other words the whole content of the image is not correctly mapped to the hash code.

Moments are set of values that best describes the content of the image[1] . Many existing system uses Zernike moments

for extracting the global features of the image [4] the reason is that Zernike moment is computationally inexpensive than legendre moments.

The proposed method use fast legendre moments to calculate hash code. The direct legendre moment is not used widely to generate hash code because it is time expensive. But with fast legendre moments the time complexity is very much reduced [21]. The two dimensional fast legendre moment function for a 2D image is computed as two, 1D function and hence the number of additions and multiplications is reduced. Further the moment's basis function can be calculated based on the size of the image and order of moment and can be stored in advance irrespective of image for fast computation.

In image self recovery, geometric moments cannot be used since the basis function $x^p y^q$ is not orthogonal. Zernike moments though they have an orthogonal basis function image reconstruction is severely handicapped due to the presence of geometric errors and approximation errors and as the moment order increases these approximation errors goes out of control. The more suitable moment for image reconstruction is legendre moments as it does not have approximation errors and image content can be extracted without any information loss [22].

II. LEGENDRE MOMENTS

Moments are set of values used to describe the information contained in the image. There are infinite numbers of moment values for obtaining the information of an image. It is very important to identify specific set of moment values that best describe the information contained in an image.

The set of direct legendre moments for a grey scale image of size M x N is given as[22]

$$L_{pq} = \sum_{i=1}^{M} \sum_{j=1}^{N} I_p(x_i) I_q(y_j) f(i,j) \text{ -- -> } 1$$

Where $f(i,j)$ is the input image and the moment kernel function is given as

$$I_p(x_i) = \frac{2p+1}{2p+2}(u_{i+1})p_p(u_{i+1}) - p_{p-1}(u_{i+1}) - (u_i)p_p(u_i) - p_{p-1}(u_i) \text{ --> } 2$$

$$I_q(y_j) = \frac{2q+1}{2q+2}(v_{j+1})p_q(v_{j+1}) - p_{q-1}(v_{j+1}) - (v_j)p_q(v_j) - p_{q-1}(v_j) \text{ ---> } 3$$

where $u_{i+1} = -i + i \vartriangle x_i$ and $u_i = -i + (i-1) \vartriangle x_i$ and $\vartriangle x_i = 2/M$

$v_{j+1} = -j + j \vartriangle y_j$ and $v_j = -j + (j-1) \vartriangle y_j$ and $\vartriangle y_j = 2/N$

The moment kernel function is independent of input image and if the size of the image and the order of moment is known then the moment kernel function can be calculated and can be stored in advanced and reused whenever needed

Eqn-1 is valid only for p≥ 1 *and* $q \geq= 1$

So the first row p=0,q=0,1,2,3…Max is calculated using

Revised Manuscript Received on October 22, 2019.

K. AliceSuresh, Assistant Professor, Department of Information Technology, Bharath Institute of Higher Education and Research, Chennai, India.

S.Thirunavukkarasu, Department of Information Technology, Bharath Institute of Higher Education and Research, Tambaram, India.

P.Kavitha, Department of Information Technology, Bharath Institute of Higher Education and Research, Chennai, India

$L_{0q} = \frac{1}{M}\sum_{i=1}^{M} \sum_{j=1}^{N} I_q(y_j) f(i,j)$----> 4

And first column q=0, p=0, 1, 2, 3…Max is calculated using

$L_{p0} = \frac{1}{N}\sum_{i=1}^{M} \sum_{j=1}^{N} I_p(x_i)\ f(i,j)$----> 5

The set of fast legendre moments for an image of size M x N can be computed as two 1D function and can be given as

$L_{pq} = \sum_{i=1}^{M} I_p(x_i) Y_{iq}$ -----> 6

where Y_{iq} is the qth order moment of row i

$Y_{iq} = \sum_{j=1}^{N} I_q(y_j) f(i,j)$ −−−>7

The image can be reconstructed without any loss of information since legendre moments are free from approximation errors and geometric errors. The image function f(x,y) can be written as an infinite series expansion in terms of the legendre polynomial over the square [-1,1] x [-1,1] is given as

$$f_{max}(x_i, y_j) = \sum_{p=0}^{\infty} \sum_{q=0}^{\infty} L_{pq} P_p(x_i) p_q(y_j) \ --> 4$$

If the order of moment is smaller than infinity then the above Eqn -4 can be rewritten as

$$f_{max}(x_i, y_j) = \sum_{p=0}^{Max} \sum_{q=0}^{p} L_{p-q,q} P_{p-q}(x_i) p_q(y_j) \ --> 5$$

where Max refers to the maximum order of moments and the total number of moments used in reconstruction of image is given as

$N_{TOTAL} = \frac{(MAX+1)(MAX+2)}{2}$

III. DIGITAL IMAGE SECURITY USING FAST LEGENDRE MOMENTS

The image of size M x N is accepted as input and image undergoes a preprocessing stage. In preprocessing the image of size M x N is converted to a fixed size of 256 x 256 using bilinear interpolation. A Gaussian filter is applied to the image to remove any additive noise. Then the image is converted to gray scale image and for this gray scale image fast legendre moments are calculated .The order of moment (p+q)=n=21. Totally 253 moments will be generated . TABLE-1 shows the set of moments of order n =10

A vector of legendre moments LM of size [1 x 253] will be generated. This vector is then normalized using function LM'=LM mod 256. This LM' describes the hash code for the input image. This hash code thus generated from image using fast legendre moments acts as a security code for the image

TABLE.1

Order	Moments	Number
0	Z_{00}	1
1	Z_{01}, Z_{10}	2
2	Z_{02}, Z_{11}, Z_{20}	3
3	Z_{03}, Z_{12}, z_{21}, Z_{30},	4
4	Z_{04}, z_{13}, z_{22}, Z_{31}, Z_{40}	5
5	Z_{05}, Z_{14}, Z_{23}, Z_{32}, Z_{41}, Z_{50},	6
6	Z_{06}, Z_{15}, Z_{24}, Z_{33}, Z_{42}, Z_{51}, Z_{06}	7
7	Z_{07}, Z_{16}, Z_{25}, Z_{34}, Z_{43}, Z_{52}, Z_{61}, Z_{70},	8
8	Z_{08}, Z_{17}, Z_{26}, Z_{35}, Z_{44}, Z_{53}, Z_{62}, Z_{71},Z_{80}	9
9	Z_{09}, Z_{18}, Z_{27}, Z_{36}, Z_{45}, Z_{54}, Z_{63}, Z_{72},$Z_{81}$$Z_{90}$	10
	Total	55

IV. SELF RECOVERY IN CASE OF TAMPERING

For any image if the security code generated various from that of actual code computed during storing the image then there may be any data change or loss of information in the image. That is this represents that the content of the image is now changed. In that case the original image can be reconstructed using Eqn-5 in which Max is equal to the order of the moment 'n'. The exact content of the image can be reconstructed using legendre moment more efficiently than Zernike moments.

V. PARAMETER SELECTION

The proposed study uses MATLAB (2013a) environment. The image dataset is calculated from internet and CASIA database [17]. The size of the image is considered to be 256 x 256, the reason being, if the size of the image is too small then the features cannot be extracted correctly and if it is too large then it increase the computational complexity. A Gaussian filter is applied to eliminate noise. Fast legendre moments are used to extract the features of the image. Since the number of additions is of O (NM^3) and multiplications is of O (M^3) this algorithm is efficient when compared with direct method.

The Euclidean distance between the actual security code (z_1) with that of computed security code (z_2) can be tolerated up to a threshold ح to allow content preserving transformation. D=||z_1-z_2|| if the distance D is less than the threshold ح then the image is considered to be unaltered. The proposed system considered ح = 7.

VI. RESULT AND DISCUSSION

The fast legendre moment for a sample matrix of size 4 x 4 A=[3 2 1 4; 2 1 3 2; 4 1 2 1; 5 2 1 2] and order 3 is calculated using the formula described in section II, and the moments L_{pq} are as shown in TABLE-2.

TABLE - 2				
L_{pq}	0	1	2	3
0	2.6875	-0.4219	1.0547	0.3486
1	-0.0469	-1.1602	0.7910	-0.4768
2	-0.3516	-0.6152	1.5381	0.1666
3	0.1299	-0.4768	-2.1918	0.7828

The Kernel generation time for fast legendre moments for various order for a image size of 64 x 64 is as shown in TABLE-3 and its graph when compared to computation time of Zernike moments and direct legendre moment is represented as shown in Figure-1.

TABLE-3			
Moment Order	Elapsed Time in sec		
	Zernike Moments	Direct Legendre Moments	Fast Legendre Moments
10	0.58155	0.0630	0.018947
20	2.0638	0.2190	0.022933
30	4.709	0.4680	0.052124
40	9.2918	0.7970	0.066111
50	12.4269	1.2500	0.083219

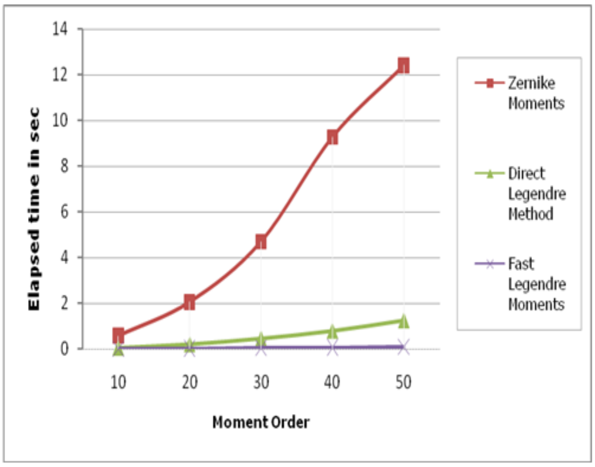

Figure-1 CPU Elapsed time for Various Moments

From Figure-1 it is clear that the Elapsed time increases with increase in moments for all the three types of moments. For fast legendre moments the elapsed time is less than one second for order up to 100 . but for Zernike moments the time increases up to 129 seconds for the same order . In terms of CPU elapsed time fast legendre moments is most efficient than Zernike moments.

The performance of reconstructed image can be analyzed using some commonly available criteria like Mean square error (MSE) and peak signal to noise ratio (PSNR). For an image of size M x N the MSE and PSNR are given as

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j-1}^{N}((f_{max}(x_i, y_j) - (f(x_i, y_j)))^2$$

$$PSNR = 10 * log_{10}(\frac{2^n - 1}{MSE})$$

The reconstruction of images for various order are as shown in Fig-2 . The MSE and PSNR for various image size and order is as shown in TABLE - 4. To improve the quality of reconstructed image histogram equalization is done at the last.

VII. CONCLUSION AND FUTURE ENHANCEMENT

In this work a security code for an image is generated using legendre moments and in case of tampering it can be reconstructed effectively using the same code. In our experiment the image security code is robust to various attacks like small angle rotation, brightness adjustments and resistance to content preserving modifications.

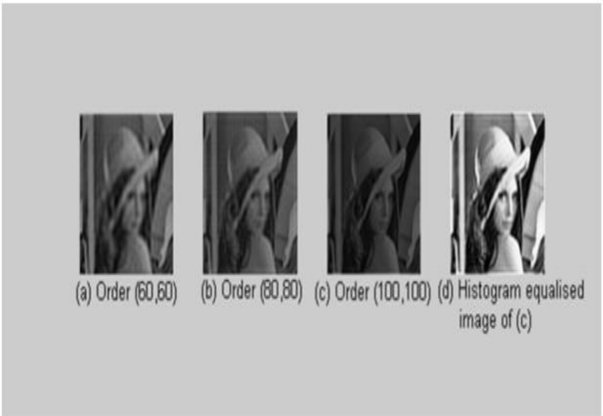

Figure-2 Reconstructed images of various order

TABLE-4		
Order	Legendre Moments	
	RE	PSNR
20	6.9188e+033	18.89
40	5.2932e+033	21.22
60	5.1486e+033	21.46
80	6.0415e+033	20.07
100	8.4332e+033	17.18

Since the moments which describe the global features of the image is only taken into consideration the generated code can miss small local information and also that the reconstruction error increase with the increase in order of moment [22] and thus the robustness of security code is greatly challenged. In future this global feature may be accompanied with content preserving local feature extraction techniques to generate code.

Conflict of Interest: Nil

REFERENCES

1. A.Haouzia, R Noumeir,"Methods for image authentication A survey" , Multimedia tools Appl 39: 1-46,Springer 2008.

2. Seyed Amir “Secure and robust two-phase image authentication”, IEEE transaction on multimedia, Vol 17, No 7, ppno 945 -956 July 2015.
3. Tri.H.Nguyen,Duc.M.Duong and Duc.A.Doung, ”Robust and High Capacity watermarking for image based on DWT-SVD”, IEEE RIVF, International conference on computing and communication Technologies Research Innovation and Vision for Future(RIVF) 2015.
4. Lima Sebatian,Abraham Varghese,Manesh.T ,” Image Authentication by content preserving robust image hashing using local and global features”,1877-0509, published by Elsevier B.V, Copyright 2015
5. M.F.Hashmi,A.R.Hambarde,A.G Keskar, “Robust image authentication based on HMM and SVD Classifiers” , Engineering letters 22: 4 El-22-4-04-Nov 2014.
6. G.L.Friedman , “ The trustworthy digital camera: Restoring the credibility to the photographic image”, IEEE Trans.Consum.Electron..Vol 39 no 4 pp 905-910, Nov 1993
7. XuLi,Xingming Sun, “ Image Integrity Authentication Scheme based on Fixed Point Theory”, IEEE trans. On Image processing Vol 24,no2 Feb 2015
8. F. Khelifi and J.Jiang, “perceptual image hashing based on virtual watermark detection,”IEEEtrans. Image process. vol. 19, no. 4, pp. 981-994, Apr.2010 V. Monga and M.K. Mihcak, ”Robust and secure image hashing via non-negative mark factorizations,”IEEE Trans. Inf. Forensics security, vol. 2, no. 3, pp. 376-390, Sep.2007
9. A.Swaminathan, Y. Mao, and m. Wu, “Robust and secure image hashing,” IEEE Trans. Inf. Forensics security, vol, 1, no. 2, pp. 215-230,Jan. 2006.
10. V. Monga, A.Banerjee, and. L. Evans, ”A clustering based approach to perceptual image hashing,” IEEE Trans. Inf. Forensics security, vol. 1, no. 1, pp. 68-79, Mar. 2006
11. Z.Tang, S.Wang, X. Zhang, W. Wei, and S.Su, “Robust image hashing for tamper detection using non-negative matrix factorization, “ J. Ubiquitous Convergence Technol., vol. 2, no. 1, pp. 18-26,May 2008.
12. S. Xiang, H. J. Kim, and J. Huang, “Histogram-based image hashing scheme robust against geometric deformations,” in proc. ACM Multimedia and security Workshop, New York,2007, pp. 121-128.
13. Y. Lei, Y. Wang, and J. Huang, “Robust image hash in radon transform domain for authentication,” Signal process. : Image commun.Vol 26, no. 6, pp. 28[8] A. Fouad and J. Jianmin, “Analysis of the security of perceptual image hashing based on non-negative matrix factorization, “IEEE Signal process. Lett. , vol. 17, no. 1, pp. 43-46, Jan. 2010.
14. R Venkatesan, SM Koon, MH Jakubowski, P Moulin. Robust image hashing.Proc IEEE IntConf Image Processing 2000;3:664-666.

AUTHORS PROFILE

K.Alice Suresh, Assistant Professor, Department of Information Technology, Bharath Institute of Higher Education and Research, India

S. Thirunavukkarasu, Assitant Professor, Department of Information Technology, Bharath Institute of Higher Education and Research, Chennai, India

P. Kavitha, Assitant Professor, Department of Information Technology, Bharath Institute of Higher Education and Research, Chennai, India