LAB BASED PROJECT

DETECTION OF COMPUTER GENERATED IMAGES

PROJECT MEMBERS:

1) JOYDEEP DAS (14116032)
2) RAVI CHANDORA (14116056)
3) SWABHIMAN PATNAIK (14116069)

Under the guidance of -

DR. VINOD PANKAJAKSHAN

Detection of Computer Generated Images

Joydeep Das (14116032) ECE, 3rd Year IIT Roorkee

Ravi Chandora (14116056) ECE, 3rd Year IIT Roorkee

Swabhiman Patnaik (14116069) ECE, 3rd Year IIT Roorkee

Abstract :

The rapid development in the field of computer graphics (CG) makes it quite easy to create photorealistic images and videos. This brings forward an emergent requirement for techniques that can distinguish CG from real contents. In this project we first differentiated between spam images and real images using intensity histogram normalization. Second is the differentiation between the real images and computer generated images i.e. animated images which are very realistic. Third is distinguishing CGI vs real person in videos using human pulse extraction method.

I.Introduction:

With the fast evolution of Computer Graphic (CG) technologies, Computer Generated Imagery is increasingly photorealistic. Many easy-to-use 3D modeling and rendering softwares such as Maya, 3ds Max, Blender etc. make it convenient for ordinary people to create special effects. This posts a new challenge for the forensic society, as it is becoming more and more difficult to distinguish CG from real contents.

CG technologies can be used by vicious groups to produce deceiving and malicious videos. Imagine the vicious ones manipulated a CG movie star to acknowledge some of his rumors, this will pollute his reputation. Even worse, it can cause social instability or international intension if a CG politician is made to make a fake statement. Motivated by the above reason, in this work, we focus on judging the authenticity of videos that include human faces.

So, First is spam image filtering. In the spam image filtering we used HSL color model which is based on intuitive color parameters. Lightness is the variable which has been used in our approach [1], under assumption that the computer generated objects will have higher lightness due to the sharpness of the objects. Image histograms were one of the main methods used to extract the color features. The color properties selected were color saturation and color histogram.

Secondly, in CGI vs real image detection, the adjacent pixel binary codes are calculated according to LTP calculations [2], and the upper and lower LTC binary codes are calculated, secondly encode in accordance to LBC encoding coding format then plotting this codes into a histogram. By histogram we will get that the PIM images are relatively changing slowly and the adjacent pixel values are relatively close while PRCG images' histograms changes relatively intensely.

Third is CGI vs real person detection, in which we first we detected the face in the video using real time face detection. Then we extracted the constant area line nose area from the face; this area is analysed by using various type of transforms and the human pulse has been analysed under fourier transform accordingly. This method is called pulse extraction method.

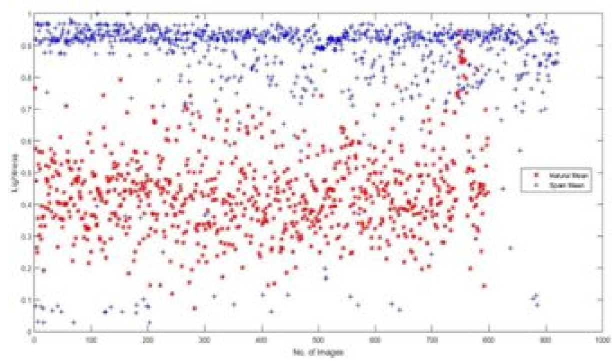
II.Analysis:

1.Spam Image Filtering :

Email Spammers now-a-days use image spam to by-pass the conventional email filters. These Spams are basically images embedded with text messages. To distinguish spam images against genuine emails, the method used depends on HSL color model, its lightness value and histogram.

There is an argument that image spam are often artificial, and contain clearer and sharper objects than legitimate images; thus, their colour distribution should be less smooth. Under assumption that in computer generated images have high lightness, especially the one used for image spam, due to the existence of light background to make it easy to read the message.

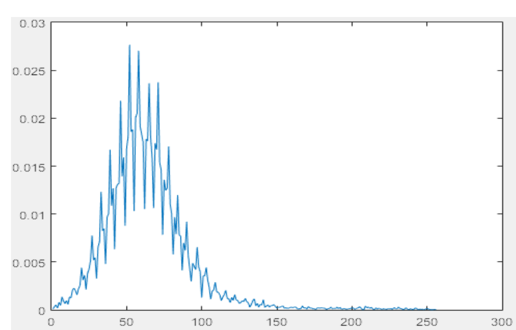
It was found that in image spam, the mean value of lightness is greater than 0.5 to make the text in the image readable, and for natural images the mean value of the lightness is between 0.2 and 0.6. as shown in Fig.3. Also it was found that the normalized lightness histogram shows peak for the color of the background, while for natural images, the distribution of colors have close values, based on that a threshold value is defined as 0.05, to differentiate and compare the components of the histograms.



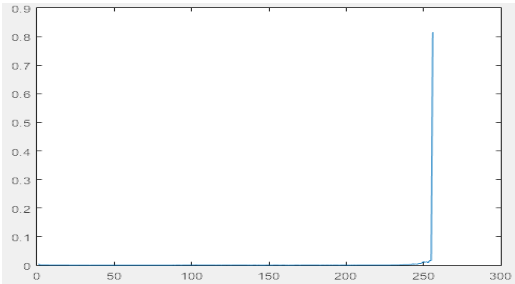
(a)Lightness Values of dataset

Differentiation strategy uses:

- rate of change = | (max*a* − max*b*) / max*b* | ×100.
  - maxa=max. histogram value before removal of all histogram bins above threshold,th= 0.05.
  - maxb= max. histogram after removal.
- If rate is more than 10% then peak is observed, it is declared as Spam Image.



(a). Natural image lightness histogram



(b). Spam image lightness histogram

2. Distinguishing general CGI vs Photographic Images

The computer generated images are detected mainly by extracting statistical characteristics of image like Higher-order wavelet statistics, Complex dimension characteristics, Statistical features of wavelet coefficients on HSV, statistical moments of wavelet sub-bands' histogram in DFT domain. We exploit the fact that PIM changes slower in brightness, colour, texture and have richer texture level than CGI.Many algorithms are proposed but all having much higher feature dimensions above 100-D. Based on less feature dimensions, LTC feature extracted ,tested on SVM and serves as good classifier between PIM and CGI.

This method uses Local Ternary Pattern (LBP) to extract the image texture features, which is based on the local binary pattern (LBP). It retains the computational efficiency, discriminatory power and noise immunity of LBP and maintains high computational complexity at the same time. in order to reduce the computational complexity and maintain a high performance, Local Ternary Count (LTC) is developed by improving LBP.

First, a window of 3x3 is created and is used to analyse the grey-level values of the neighbouring pixels. The binary codes are calculated and the upper & lower LTC binary codes are obtained from the binary code. A histogram was plotted for the different LTC values (0-8). Each bar of the histogram is a feature. Three histograms were plotted for each domain of the HSV plane. So, the total number of features used for training 9x3x2 = 56. This method is applied on a dataset of CG images and photographic images. SVM was used to classify the images as CG or real.

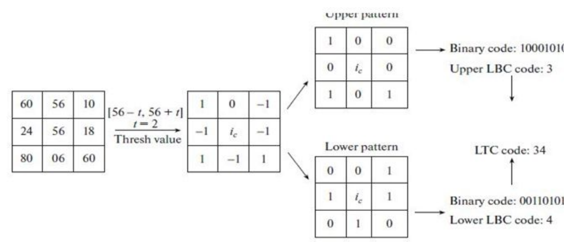
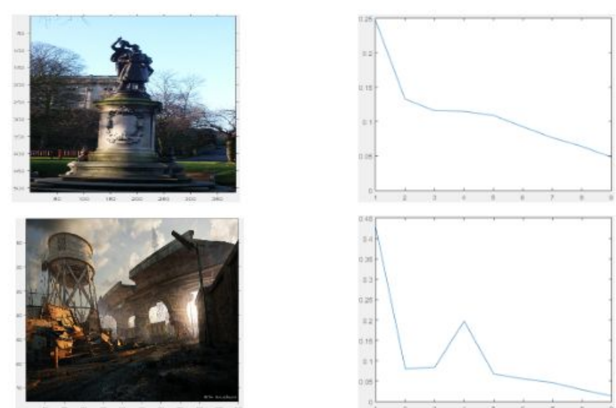


Fig3.



(a). Natural Image and its Histogram (b). CGI Image and its Histogram

3. Detecting CG faces in videos

This method uses human pulse signal to distinguish between CG and real videos [6] that include human faces. We use a robust tracking method to locate a patch of skin on the face. Robust tracking method is used to locate a constant patch of skin on the face, a Viola-Jones for Bounding-Box. Then, a chrominance-based algorithm is employed to robustly extract pulse signal. By checking the frequency waveform of the extracted pulse signal, we can tell CG and real videos apart.

A. Extraction of ROI region:- This can be directly obtained using Bounding-Box function of matlab for constant face region like nose,forehead. We have considered nose ROI for our case.
B. Pulse Extraction:- Based on the tracked ROI in each frame, we average the intensity value of all pixels in the ROI for each of the RGB channel to get the raw RGB signal according to this formula, where Cn belongs to {Rn,Gn,Bn}. Here length n includes at least one human pulse.

$$C_{ni} = \frac{\sum_{j=-n}^{n} C_{i+j}}{2n+1}$$

Then we use a chrominance-based method proposed in [14] to extract the pulse signal. The pulse extraction method is based on a sophisticated light reflection model of human skin.The influence of head motion is seen as an equal intensity modulation for all channels. Hence, pulse
signal can be got from chrominance components to suppress motion noise. The extracted pulse signal is in the form of a linear combination of the bandpass filtered and normalized raw RGB signal. Two chrominance signals are defined as,

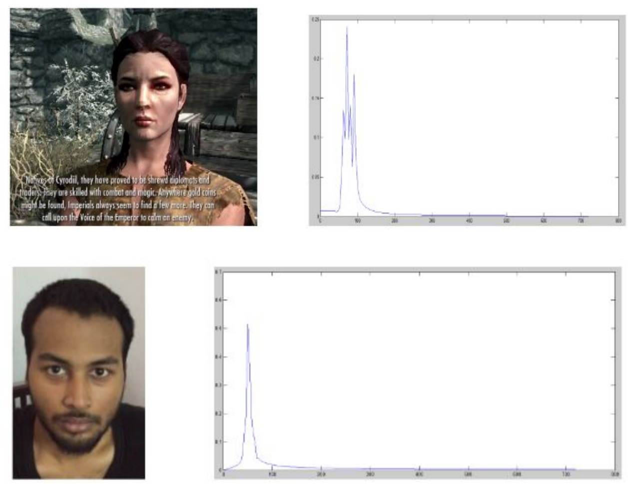
$$X = 3R_n - 2G_n$$

$$Y = 1.5R_n + G_n - 1.5B_n$$

X, Y is then bandpass filtered to get Xf, Yf . Then the pulse signal S is obtained, where α is the ratio of the standard deviations of Xf and Yf.

$$S = X_f - \alpha Y_f$$

we set the passband for bandpass to 50 ~ 80 bpm which corresponds to the range of normal human pulse rate. In pulse signal S, we apply Frequency transform to observe that the pulse for human shows a sharp peak but for computer generated it gives arbitrary peak values with arbitrary number of maximas.



(a). CGI Face and its Pulse (b). Real Face and its Pulse

III. RESULTS:

1.Spam Images vs Non-Spam Images:

The two features were tabulated - lightness mean and rate of change. On the basis of these two features the images were classified. Two approaches were taken :-

1. Direct Method

The two features were directly compared with threshold values i.e. (Rate of change > 10%) && (Lightness mean > 0.5)

If this condition was true then the image was declared as spam or else photographic image. The results obtained from using this predicate were satisfactory.

- True positive rate = 93.27%
- True negative rate = 92.61%
- False negative rate = 06.73%
- False positive rate = 07.39%

2.Supervised Method -

The system was trained randomly on 80% data of Spam image dataset (921 images) and natural dataset (798 images) using the SVM trainer in MATLAB.

Then the remaining 20% dataset were tested with the trained program. The results were similar to the previous method -

- True Positive rate = 97.1 %
- True Negative rate = 91.35%.

2. CGI Photo-Realistic Image Vs. Photographic Image.

Natural Image dataset Contains ucid database[5] (1338 images) and CGI are downloaded from www.raph.com and www.irtc.org.(250 images).

The SVM accuracy obtained from this method is :-

- True Positive rate - 95.26%.
- True Negative rate - 99.54%.

This method is further extended to detect Computer generated videos by making a SVM structure of test-train model with train data taken from both Photographic and Photorealistic images.For training ,from a video we select the maximum standard deviation image as it contains the most information about an image. Then this classifier is tested against randomly collected data from testing image and a good percentage of accuracy is obtained.

- True Positive rate - .90%
- True Negative rate - 87%.

3. Genuine Faces Vs CG Faces:

In this method, after analyzing the pulse signal in frequency domain we developed a novel method to distinguish CG vs Genuine by detecting normalized difference between first and second peaks and then normalizing with respect to second peak. The results shows if it’s greater than 1 than real or else CG face. It has been tested on 8 Real and 8 CGI Images and the result is shown below.

For bandpass filter design in matlab code with N order filter and lower frequency f1 and higher frequency f2 and sampling frequency fc we get (N,f1,f2,fs) as shown,

```
%% filter
d=fdesign.bandpass('N,F3dB1,F3dB2',20,5/6,8/6,29.97);
Hd=design(d,'butter');
```

Fig. Matlab Code

- For Forged Videos:-

Serial no.	Frame rate	1st Highest peak (x)	2nd Highest peak (y)	(x-y)/y
1	21.2	0.0235	0.011	1.091
2	21.2	0.35	0.24	0.45
3	20.9	0.36	0.22	0.63
4	19.8	0.21	0.115	0.82
5	19.9	0.32	0.26	0.23
6	20.8	0.245	0.215	0.319
7	20.6	0.27	0.19	0.42

- For Genuine Videos:-

Serial no.	Frame rate	1st Highest peak (x)	2nd Highest peak (y)	(x-y)/y
1	29.97	0.5	0.007	70.4
2	29.97	0.16	0.05	2.2
3	29.97	0.16	0.14	0.14
4	29.97	0.51	0.04	11.75
5	29.97	0.62	0.25	1.48
6	29.97	0.19	0.04	3.75
7	29.97	0.34	0.02	16

IV.Conclusion:

The field of CGI detection has seen many rapid strides in the last few years, and still research is being carried on. With this project we tried to create an arsenal of methods to deal with most of the computer generated forgeries like spams, CG images, rich texture images, face videos, and general videos. All the methods implemented had decent accuracy of 90% and above. The first method deals with SPAMs, second one deals with general CGIs and its extension deals with videos with CG scenes. The last paper detects forgery in faces present in videos.

V.References:

[1] Hazza, Zubaidah Muataz, and Normaziah Abdul Aziz. "Detecting computer generated images for image spam filtering." Advanced Computer Science Applications and Technologies (ACSAT), 2012 International Conference on. IEEE, 2012.

[2]Tan, D. Q., et al. "Detecting computer generated images based on local ternary count." Pattern Recognition and Image Analysis 26.4 (2016): 720-725.

[3]Peng, Bo, et al. "Detection of computer generated faces in videos based on pulse signal." Signal and Information Processing (ChinaSIP), 2015 IEEE China Summit and International Conference on. IEEE, 2015.

[4]de Haan, Gerard, and Vincent Jeanne. "Robust pulse rate from chrominance-based rPPG." IEEE Transactions on Biomedical Engineering 60.10 (2013): 2878-2886.

[5] G. Schaefer and M. Stich, “UCID - An uncompressed colour image database,” in Proc. SPIE, Storage and Retrieval Methods and Applications for Multimedia, San Jose, 2004.

[6] Image Spam Hunter, Yan Gao, Ming Yang and Xiaonan Zhao EECS Department, Northwestern University, http://www.cs.northwestern.edu/~yga751/ML/ISH.htm.