

Analyzing the Real Photo Images with the Scanned Photo Images using Histogram Equalizer

Dr.M.Malathy¹, Mr.Vijayanand², Dr.Arputha Vijaya Selvi³

¹Professor, Dept. of CSE, RRCE, ²Associate Prof., Dept. of CSE, ACSCE, VTU, Bangalore-74. ³Dean R&D, KCE,TamilNadu.
anandanmalathy@gmail.com, ksgvanand@gmail.com, vijayas_02@yahoo.co.in

ABSTRACT- In the biometric world, image analysis places the important role. The real acquired images are forged by the scanned photo images. Unauthorized malicious user may try to use the authorized person's scanned photo images for the access process. An authentication system should analysis difference between the real images and the scanned photo images. This paper is mainly focused on analyzing the real acquiring images with scanned photo images using histogram equalizer.

Keywords: Real acquired images, Scanned photo images, Histogram Equalizer.

I. INTRODUCTION

Recent security world, Biometric authentication system is facing the treats, vulnerabilities by the attackers. In generic biometric system has attacked by the attacker in the acquiring level, preprocessing level, feature level, database storage level, matching level and communication level. Figure 1.1 describes the basic concept of biometric attacks in various levels. Spoofing the images using synthesized images is one point of view. Synthesizing images is the reverse process of the recognition or authentication system. Analyzing the images is the forward process of the recognizing or authentication system. Sometime printed images are used to forge the authentication system. Analyzing the image in the acquiring level is place the important role to detect the unauthorized access in the access level itself. Acquiring devices like camera, sensors are not detecting the forge images. Hardware level attacking may be done in the acquiring level itself. So this image analysis is mainly focused on the acquired image is real or forged image.

The biometric authentication process compares a registered or enrolled biometric sample i.e. biometric template or identifier against newly captured biometric images.

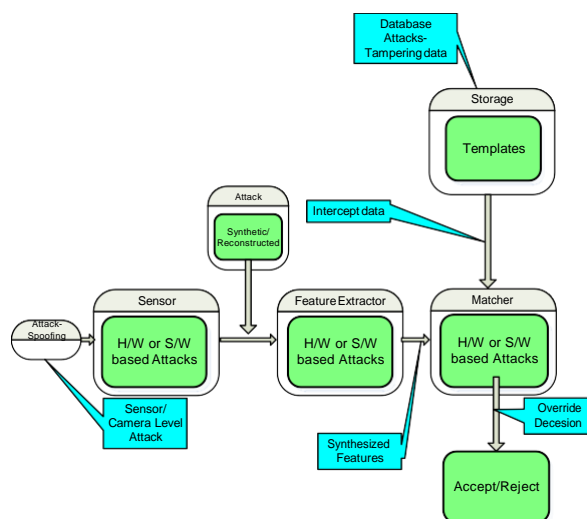


Figure 1.1 Biometric Attacks

Here, the user enters their identity to the biometric system. While entering the individual biometric traits like face, the vulnerabilities such as spoofing, collusion and coercion are occurred. The biometric system contains sensor/matcher limitations and the individuality of the biometric traits as intrinsic failure. The entered biometric traits are stored in the biometric database to provide better application/ services. The individual biometric traits are affected by the enrollment of fraud steal and made modification in the biometric images. Different types of vulnerabilities are occurred while performing this type of modification done in the enrollment.

II. RELATED WORKS

Malathy M & Arputha V.Selvi [1] have proposed, the Spoofed Iris Recognition: Synthesis of Gabor and LBP descriptor using SPPC, from this paper, the robustness of iris recognition system with spoofing attack is explained. This algorithm is a combination of Gabor wavelet followed by local binary pattern description (LBP) where the magnitude coefficient from Gabor wavelets takes as its input. Both dataset iris images and spoofed iris images are assessed by the algorithm in order to rise a genuine acceptance ratio (GAR)[1].Malathy M & Arputha V.Selvi [2] have proposed, 2-DWT and AES: Secure Authentication Management for Polar Iris Templates Using Visual Cryptography, from this paper, to protect the iris template against the spoofing attacks in the database storage level. Two shares were stored separately and merging the shares then only authentication system accessed the genuine user. Malathy M & Arputha V.Selvi [3] have proposed, the liviness face detection based on the binary image of the eye images. These eye images are cropped from the face images and photo face images, the gray scale value of the photo eye image had converted in to binary images and found the liviness. Akhtar, et al [4] have investigated, a real spoof attack samples that verify the multimodal biometric systems. Spoofed face and iris samples were replicated with a photo attack method. The photo of each individual was put in front of the capture device. While spoofed fingerprint samples was created by the same method. For each individual, 10 spoofed face, fingerprint and iris samples were created. The biometric systems were not intrinsically robust against spoof attacks contrary to the common belief. It can be cracked by spoofing only one biometric trait. Schwartz, et al[5] have presented a

face spoofing detection through partial least squares and low-level descriptors. Partial Least Squares regression to provide a feature weighting to distinguish between live and spoof images or videos. The use of a robust set of feature descriptors renders many classical machine learning methods intractable due to extremely large resulting feature space, which becomes more evident when the temporal function was considered. The reduced number of training samples was compared to the number of descriptors.

III. PROPOSED IMAGE ANALYZER

In the proposed Image analyzer, the real face image and the scanned photo image were analyzed according to the variations in the histogram equalizer. The Fig 1.2 shows the system architecture of the image analyzer. It has two modules. One is acquiring the face image in the different type of devices. The face image captured from the webcam and stored it in the system. The photo face image scanned from the scanner and stored it in the system. The both images are given to the input of the image analyzer. The analyzer has to find the contrast of images using the histogram equalizer. The histogram equalizer, the image is divided in to two frames horizontally vertically row and col of the pixel intensity taken to find the cumulative sum of the image. The contrast, correlation, energy and homogeneity are found by the image analyzer based on the following equations, Eq.No.(1) represents the mathematical equation of the contrast.

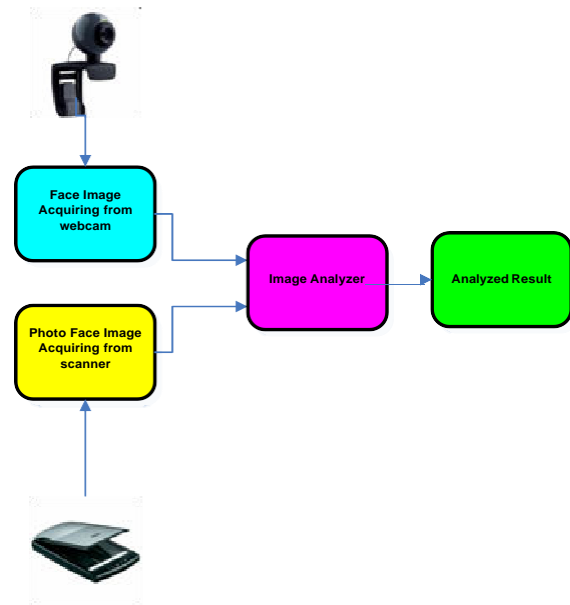


Fig.1.2 System Architecture of Image Analyzer

$$\text{Contrast} = \sum_{(i,j)} [i-j]^2 P(i,j) \dots\dots\dots (1)$$

Where p=image, i,j=coordinates , p(i,j)=Intensity value at i,j

Eq.No.(2) represents the mathematical equation of the correlation.

$$\text{Correlation} = \sum_{(i,j)} P(i,j) \left[\frac{(i-\mu)(j-\mu)}{\sqrt{(\sigma)^2(\sigma)^2}} \right] \dots\dots\dots (2)$$

Eq.No.(3) represents the mathematical equation of the Energy.

$$\text{Energy} = \sum_{(i,j)} P(i,j)^2 \dots\dots\dots (3)$$

Eq.No.(4) represents the mathematical equation of the Homogeneity.

$$\text{Homogeneity} = \sum \frac{P(i,j)^2}{1+(i-j)} \dots\dots\dots (4)$$

The final result, the differences of the values of all the parameters are found and using these different values analysis shown the original and fake images are found for an authentication system.

IV. IMPLEMENTATION RESULT

The implementation results are given below. The Fig. 1.3 shows the Original webcam image that corresponding histogram image and also histogram equalized image with the corresponding histogram equalized image.

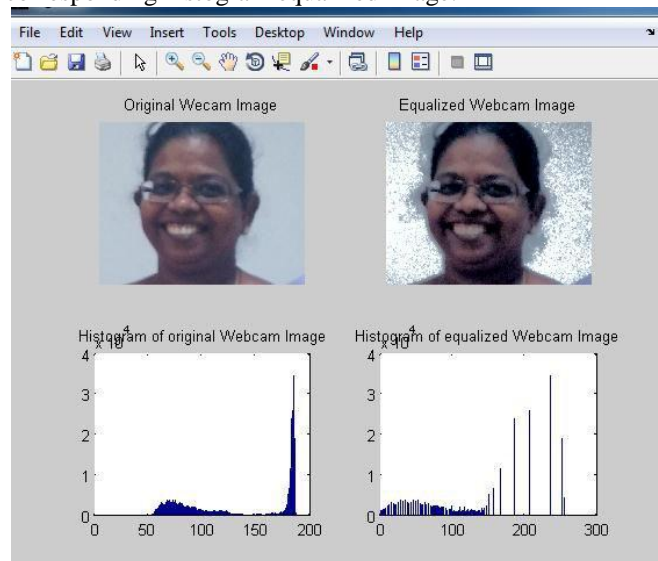


Fig. 1.3 Webcam image with the corresponding histograms

The Fig. 1.4 shows the Scanned photo image that corresponding histogram and also histogram equalized scanned photo image with the corresponding histogram equalized image.

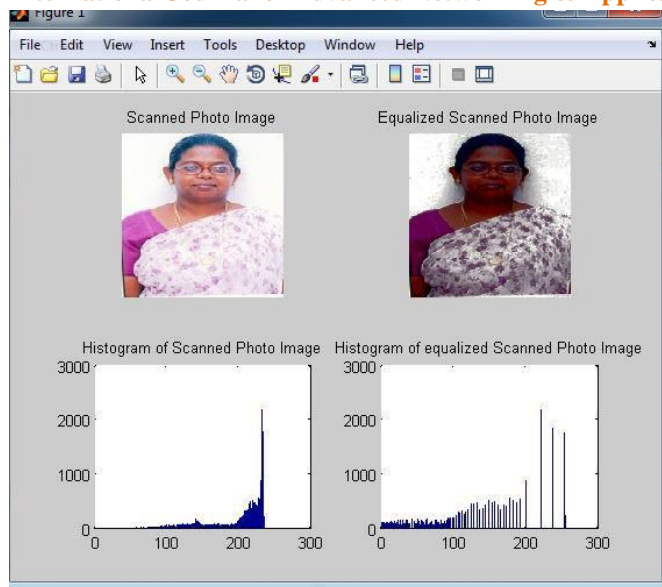




Fig. 1.4 Scanned photo image with the corresponding histograms

Table 1.1 Difference between the parameters of scanned photo image and the real photo image

Sl. No	Type of the Images	Images	Contrast	Correlation	Energy	Homogeneity
1	Scanned Photo Image		0.239	0.945	0.198	0.907
2	Real Photo Image		0.036	0.992	0.321	0.982
Difference =(Real Photo image - Scanned photo image)			-0.203	0.047	0.123	0.075

The table 1.1 shows the different between the parameters of the two types of images.

V. CONCLUSION

Comparison of two face images, one is webcam face image, another one is scanned face image, both inputs are given to the image analyzer, the image analyzer analysis the images based on the histogram equalizer. Finally, conclude that the parameters differences are, contrast is -0.203, correlation is 0.047, energy is 0.123 and homogeneity is 0.075. Based on the results the two images are different. It will useful to

identify the original and fake images in the authentication system. In future work, database should be increase and train the image analyzer to find the printed photo image, all type of original and fake biometric images.

REFERENCES

- [1] Malathy, M & Arputha Vijaya Selvi, J., 'Spoofed Iris Recognition: Synthesis of Gabor and LBP descriptor using SPPC', Australian Journal of Basic and Applied Sciences (ISSN 1991-8178), pp. 433-442. 2014
- [2] Malathy, M. & Arputha Vijaya Selvi, J., '-2-DWT and AES: Secure Authentication Management for Polar. Iris Templates Using Visual Cryptography', Journal of Testing and Evaluation, Vol. 45, No. 2, 2017, pp. 1-2015; published online February 2, 2016.
- [3] Malathy, M & Arputha Vijaya Selvi, J., 'Face Liveness Authentication/Anti-Spoofing Engine using Morphological- shared weight Neural Network', Advances in Mathematics Scientific Developments and Engineering Application, Narosa Publishing House Pvt.Ltd., , ISBN-978-81-8487-074-9, pp.550-557. 2010
- [4] Akhtar, Zahid, and Sandeep Kale. "Security Analysis of Multimodal Biometric Systems against Spoof Attacks." Advances in Computing and Communications. Springer Berlin Heidelberg, 2011. 604-611.
- [5] Schwartz, William Robson, Anderson Rocha, and Helio P. Edrini. "Face spoofing detection through partial least squares and low-level descriptors." Biometrics (IJCB), 2011 International Joint Conference on. IEEE, 2011.
- [6] Heo, Jingu, and Marios Savvides. "Gender and ethnicity specific generic elastic models from a single 2D image for novel 2D pose face synthesis and recognition." Pattern Analysis and Machine Intelligence, IEEE Transactions on 34.12 (2012): 2341-2350.
- [7] Malathy M & Arputha Vijaya Selvi J, '-Survey of Cyber Security and Laws for Social Media Sites (SMS)', Proceedings of International Conference on Emerging Trends in Engineering, Technology and Science (ICETETS-2016) at Kings College of Engineering, Thanjavur India, 978-1-4673-6725-7/16/213-216 ©2016 IEEE
- [8] Malathy, M & Arputha Vijaya Selvi, J 2012, 'Multimodal Biometric Decision Fusion for Liveness Authentication / Anti-Spoofing Engine', Electronic Design and Signal Processing Narosa Publishing House Pvt.Ltd., ISBN 978-81-8487-160-9, pp.195-201.
- [9] Feng, Zhen-Hua, et al. "Random cascaded-regression cope for robust facial landmark detection", IEEE Signal Processing Letters 1.22 (2015): 76-80.
- [10] M. Malathy & J. Arputha Vijaya Selvi, J 2011, 'Multimodal Biometric Expert Decision Fusion', International Journal of Mathematics, Computer Sciences and Information Technology Vol. 4, No. 1, January-June 2011, pp. 113-123.