AUTHENTICITY ALERT SYSTEM USING RASPBERRY-PI BASED FEATURE APPRECIATION IN SCRAMBLED DOMAIN

G.S.SIVA KUMAR [1], G.PRUDHVIJA[2]

[1]G.S.Siva kumar, M.Tech (I&CS). Assoc.Professor, Dept of ECE, pragati engineering college, surampalem, East Godavari Dist., A.P., India.

[2] G.Prudhvija **,** M.Tech Student, Dept of ECE, pragati engineering college, surampalem, East Godavari Dist, A.P., India.

Abstract:

With the rapid development of internet-of-things (IoT), face scrambling has been proposed for privacy protection during IoT-targeted image/video distribution. Consequently in these IoT applications, biometric verification needs to be carried out in the scrambled domain, presenting significant challenges in face recognition. Since face models become chaotic signals after scrambling/encryption, a typical solution is to utilize traditional data-driven face recognition algorithms. While chaotic pattern recognition is still a challenging task, in this paper we propose a new ensemble approach – Many-Kernel Random Discriminant Analysis to discover discriminative patterns from chaotic signals. We also incorporate a salience-aware strategy into the proposed ensemble method to handle chaotic facial patterns in the scrambled domain, where random selections of features are made on semantic components via salience modelling. The experimental results successfully demonstrate that the proposed scheme can effectively handle chaotic signals and significantly improve the recognition accuracy In our experiments, the proposed MK-RDA was tested rigorously on three human face datasets: the ORL face dataset, the PIE face dataset and the PUBFIG wild face dataset making our method a promising candidate for secure biometric verification in emerging based on IoT applications

Keywords*: GSM, USB camera, LAN, Raspberry-pi.*

Introduction:

Compared with full encryption methods, face scrambling is a compromise choice because it does not really hide information, since unscrambling is usually achievable by simple manual tries even though we do not know all the parameters. It avoids exposing individual biometric faces without really hiding anything from surveillance video. As shown in Refs.[5~14], scrambling has recently become popular in the research field of visual surveillance, where privacy protection is needed as well as public security. Another advantage of face scrambling over encryption is its computing efficiency, and usually it is far simpler than complicated encryption algorithms. In many business cases such as public surveillance, the purpose is limited to only privacy protection from unintentional browsing of user data. Hence, full encryption becomes unnecessary in this context. There are many ways to perform face scrambling. For example, scrambling can be done simply by masking or cartooning [8]. However, this kind of scrambling will simply lose the facial information, and hence subsequent face recognition or verification becomes unsuccessful in this case. Especially for security reasons, it is obviously not a

good choice to really erase human faces from surveillance videos. In comparison, the Arnold transform [13, 14], as a basic step in many encryption algorithms, is a kind of recoverable scrambling method. Scrambled faces can be unscrambled by several manual tries. Hence, in this work, we have chosen Arnold transform based scrambling as our specific test platform. Face recognition has been extensively researched in the past decade and significant progress has been seen towards better recognition accuracy in recent reports [15~21]. These approaches usually exploit semantic face models [22~23] where a face is considered as an integration of semantic components (such as eyes, nose and mouth), and hence semantic related sparse features or local binary patterns (LBP) can be effectively used to improve the recognition accuracy.

LITERATURE SURVEY

Fake biometrics means by using the real images like iris images captured from a printed paper or fingerprint captured from a dummy finger of human identification characteristics create the fake identities like fingerprint on printed paper. Fake user first captures the original identities of the genuine user and then they make the fake sample for authentication. There is no such technology to provide security for fake users. In the proposed method, we present a novel software-based fake detection method that can be used in multiple biometric systems to detect different types of fraudulent access attempts. The objective of the proposed system is to enhance the security of biometric recognition frameworks, by adding liveness assessment in a fast, user-friendly, and non-intrusive manner, through the use of image quality assessment. Here we are interfacing camera to ARM RAPBERRY-PI. The camera will capture face image of a person and send to RASBERRY-PI. The RAPBERRY-PI will recognize the face of the particular person from the image. If they are matched then it will display the data on display unit and send to email. Otherwise it will send the message to the police or authorized one about wrong accessing and send to email.

PROPOSED SYSTEM

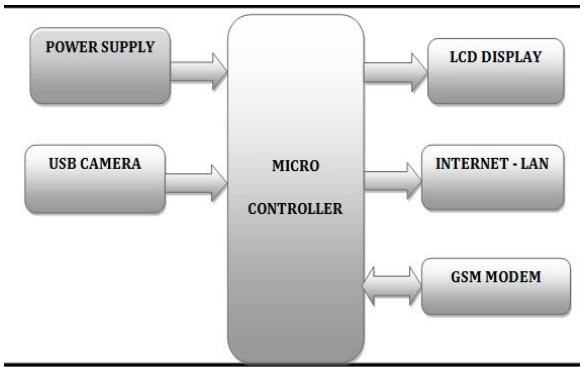

Fig:1:Block diagram

METHODOLOGY

Micro controller: This section forms the control unit of the whole project. This section basically consists of a Microcontroller with its associated circuitry like Crystal with capacitors, Reset circuitry, Pull up resistors (if needed) and so on. The Microcontroller forms the heart of the project because it controls the devices being interfaced and communicates with the devices according to the program being written.

Liquid-crystal display (**LCD**) is a flat panel display, electronic visual display that uses the light modulation properties of liquid crystals. Liquid crystals do not emit light directly. LCDs are available to display arbitrary images or fixed images which can be displayed or hidden, such as preset words, digits, and 7-segment displays as in a digital clock.

GSM:

Global System for Mobile Communication (GSM) is a set of ETSI standards specifying the infrastructure for a digital cellular service.The network is structured into a number of discrete sections.Base Station Subsystem – the base stations and their controllers explained

Network and Switching Subsystem – the part of the network most similar to a fixed network, sometimes just called the "core network"
GPRS Core Network – the optional part which allows packet-based Internet connections
Operations support system (OSS) – network maintenance.SM was intended to be a secure wireless system. It has considered the user authentication using a pre-shared key and challenge-response, and over-the-air encryption. However, GSM is vulnerable to different class of attacks, each of them aiming a different part of the network.

Fig:2: GSM Module

WEBCAM

"Webcam" refers to the technology generally; the first part of the term ("web-") is often replaced with a word describing what can be viewed with the camera, such as a netcam or streetcam. Webcams are video capturing devices connected to computers or computer networks, often using USB or, if they connect to networks, Ethernet or Wi-Fi. They are well-known for low manufacturing costs and flexible applications. Video capture is the process of converting an analog video signal—such as that produced by a video camera or DVD player—to digital form. The resulting digital data are referred to as a digital video stream, or more often, simply video stream. This is in contrast with screen casting, in which previously digitized video is captured while displayed on a digital monitor

Webcams typically include a lens, an image sensor, and some support electronics. Various lenses are available, the most common being a plastic lens that can be screwed in and out to set the camera's focus. Fixed focus lenses, which have no provision for adjustment, are also available. Image sensors can be CMOS or CCD, the former being dominant for low-cost cameras, but CCD cameras do not necessarily outperform CMOS-based cameras in the low cost price range. Consumer webcams are usually VGA resolution with a frame rate of 30 frames per second. Higher resolutions, in mega pixels, are available and higher frame rates are starting to appear.

Fig:3: Webcam

The video capture process involves several processing steps. First the analog video signal is digitized by an analog-to-digital converter to produce a raw, digital data stream. In the case of composite video, the luminance and chrominance are then separated. Next, the chrominance is demodulated to produce color difference video data. At this point, the data may be modified so as to adjust brightness, contrast, saturation and hue. Finally, the data is transformed by a color space converter to generate data in conformance with any of several color space standards, such as RGB and YCbCr. Together, these steps constituted video decoding, because they "decode" an analog video format such as NTSC orPAL.Support electronics are present to read the image from the sensor and transmit it to the host computer. The camera pictured to the right, for example, uses a Sonix SN9C101 to transmit its image over USB. Some cameras - such as mobile phone cameras - use a CMOS sensor with supporting electronics.

FEATURES:

- Smallest wireless video & audio camera
- Wireless transmission and reception
- High sensitivity
- Easy installation & operation
- Easy to conceal
- Light weight
- Low power consumption
- Small size

SPECIFICATIONS:

- Output frequency: 900MHZ 1200MHZ
- Output power: 50mW 200mW
- Power supply: DC +6~12v
- Distance covered: 10m

CONCLUSION

In conclusion, we have identified a new challenge in scrambled face recognition originated from the need for biometric verification in emerging IoT applications, and developed a salience-aware face recognition scheme that can work with chaotic patterns in the scrambled domain. In our method, we conjectured that scrambled facial recognition could generate a new problem in which “many manifolds” need to be discovered for discriminating these chaotic signals, and we proposed a new ensemble approach – Many-Kernel Random Discriminant Analysis for scrambled face recognition. We also incorporated a salience-aware strategy into the proposed ensemble method to handle chaotic facial patterns in the scrambled domain, where random selection of features is biased towards semantic components via salience modelling.

REFERENCES

[1] Singh, A. ; Karanam, S. ; Kumar, D. "Constructive Learning for Human-Robot Interaction", IEEE Potentials, Vol 32, Issue 4, 2013, Page(s): 13 – 19.

[2] Jayatilake, D. ; Isezaki, T. ; Teramoto, Y. ; Eguchi, K. ; Suzuki, K. "Robot Assisted Physiotherapy to Support Rehabilitation of Facial Paralysis", IEEE Trans Neural Systems and Rehabilitation Engineering, Vol. 22 , Issue 3,

[3] McDuff, D. ; Kaliouby, R.E. ; Picard, R.W. "Crowdsourcing Facial Responses to Online Videos", IEEE Trans Affective Computing, Vol 3, Issue 4, 2012 , Page(s): 456 – 468

[4] Fleck, S.; Strasser, W. "Smart Camera Based Monitoring System and Its Application to Assisted Living", Proceedings of the IEEE, On page(s): 1698 - 1714 Volume: 96, Issue: 10, Oct. 2008

[5] A. Melle, J.-L. Dugelay, "Scrambling faces for privacy protection using background self-similarities," Proc. 2014 IEEE International Conference on Image Processing (ICIP), 2014, pp.6046-6050.

[6] Z. Erkin, M. Franz, J. Guajardo, S. Katzenbeisser, I. Lagendijk, T. Toft, "Privacy-Preserving Face Recognition," Proc. Ninth Int'l Symp. Privacy Enhancing Technologies (PETS '09), 2009, pp.235-253.

[7] T. Honda, Y. Murakami, Y. Yanagihara, T. Kumaki, T. Fujino, "Hierarchical image-scrambling method with scramble-level controllability for privacy protection," Proc. IEEE 56th International Midwest Symposium on Circuits and Systems (MWSCAS), 2013, pp.1371-1374.

[8] A. Erdlyi, T. Bart, P. Valet, T. Winkler, B. Rinner, "Adaptive Cartooning for Privacy Protection in Camera Networks". Proc. International Conference on Advanced Video and Signal Based Surveillance, 2014, pp.6.

[9] F. Dufaux, T. Ebrahimi, "Scrambling for Video Surveillance with Privacy," Proc. 2006 Conference on Computer Vision and Pattern Recognition Workshop, Washington, DC, USA, 2006, pp.106-110.

[10] F. Dufaux, "Video scrambling for privacy protection in video surveillance: recent results and validation framework," Proceedings of SPIE, Vol. 8063, 2011, pp.14.