An Authentication Technique using Fractal Recognition and RFID

D.C. Jullie Josephine*, K.G. Saravanan
Department of CSE, Kings Engineering College, Chennai.
***Corresponding author: E-Mail: drdcjulliejosephine@gmail.com**

ABSTRACT

An advancements in technology leads to critical issues like unauthorized access in the banks and other public sectors become a prime factor. To overcome this kind of problems, we need a lot of techniques in the security evaluation. Processing huge data for providing secure access becomes more challenging fact. This includes clear technical advancement in individual person identification along with clear data processing and immediate response embedded with authentication mechanism like RFID cards. Hence we devise a system to do the fractal recognition for each entity. Fractal recognition technique is a filtering mechanism, it filters the input the input and finally a verification mechanism to identify the individual person is authentic or not.

KEY WORDS: RFID, IFS.

I. INTRODUCTION

In the last few decades the usage of this technology is in implementation in various fields like Defense, Environment, Health Care, Agriculture, Corporate, the main purpose of using RFID is for security evaluation i.e. to find the authorized person although in few cases RFID is also implemented for tracking products and analyzing the travel patterns through continues monitoring of sensor data. For example consider monitoring the persons who access to confidential rooms in a corporate office. It is tedious job even if we monitor through security cams or manual checking of each individuals. It would consume lot of time and human resources hence it's less efficient. In same environment if we use an RFID circuit, all the authorized persons are registered one time only. Then every time the person needs access he can just use his RFID to verify himself. The risk factor in this process is that what if the authorized person loses his RFID or in worst cases an anonymous person gets the RFID of a registered user and uses it to get access to the information. To overcome this issue we embed the Fractal recognition in the system which needs the registered users to verify their face each time they need a access. Now consider the same corporate company example hence we embedded fractal recognition even if an unauthorized person gets the RFID of an registered user he cannot get access since he can't produce the face of the registered user. The performance measure of the security evaluation system is now increased.

Background:

RFID: RFID stands for Radio-Frequency Identification. The RFID device provides a unique identifier for that object. There are two types of device active and passive device. In addition, the RFID tag may be. Active RFID tags have own power source and can get the signal even from far distance. They have limited life spans. Passive RFID tags, is smaller and have a unlimited life span.

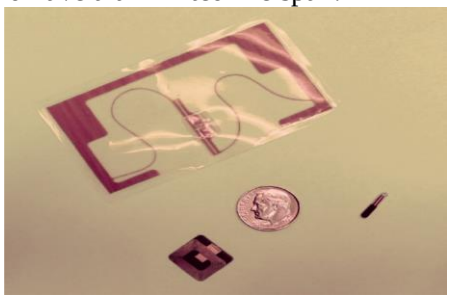

Figure.1. RFID Card

Figure.2.RFID Circuit

Fractal Detection and Recognition: The approach scans the input image fully and identifies the face by basic filtering process this methodology helps in reduction of pixel manipulation, computation and storage cost at the same without losing the performance factors.The algorithm we used in this system identifies the fractal and recognize the image with greater accuracy.

Fractal Image Encoding: IFS of an image are calculated by dividing the image into blocks. The blocks will not overlap.

- The image is divided into blocks of size $C_{max} \times C_{max}$, and named as range blocks.
- The non-overlapping blocks of size $E_{max} \times E_{max}$, named domain blocks, usually E max = 2Cmax.
- Block E_i, of size $E_{max} \times E_{max}$ is transformed and by gray value and the variance of block E_i. Next, search for the block E_i which can match block R_i best from the same class of block R_i and compute the *rms* between the best matching block E_i and block R_i. If the *rms* value is less than the given value, the related parameters are recorded.
- End.

Face Image Recognition: Experiment Steps: The image of record is the input image, and database contains *n* images known as encoding dictionary. The image of record is encoded by an encoding dictionary, b which then provides *n* ".dat" files.

- The *n* ".dat" files are iterated five times by the fractal image decoding program, which provides *n* decoding images.
- The method of image recognition:

The PSNR is the peak signal-to-noise. It is defined as ratio between the image of record and the decoding image. The images whose PSNR value is greater than the threshold value are the recognized images. If all PSNR values are less than the threshold value, then there is no image of the same person with an image of record in the face image database.

We then compute the PSNR,

$$PSNR = 10 \log_{10} \frac{M \times N \times 255^2}{\sum_{m,n} (S_{m,n} - S'_{m,n})}$$

$S_{m,n}$ is defined as the gray value of the image in record, $s_{m,n}$ is the gray value of the decoding image in the database, *M* is height of the image, *N* is the width of the image. The image is close to original image because the PSNR value is close to given value.

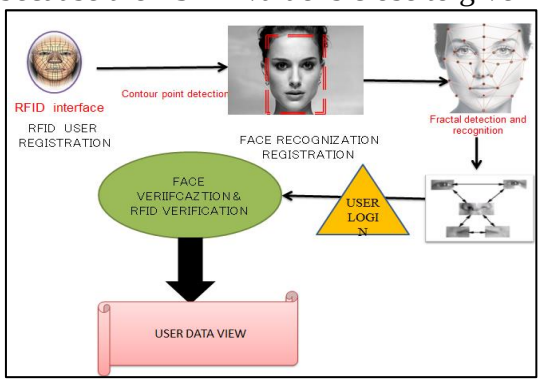

Figure.3. Architecture

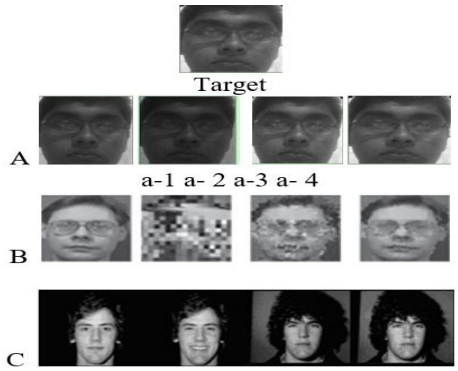

Figure.4. Image database

Table.1. PSNR calculations

	Image (a-4)/ Image A	Image (b-4)/ Image A	Image (c-4)/ Image A
PSNR	24.215244	14.437908	17.738887

As shown in Table.1, since the PSNR between image (a-4) and Image A is the highest, image (a-4) is obviously the recognized image of Image A. After comparing the PSNR value b-4 and c-4 and found to be less, they are not recognized as target image.

2. EXPERIMENTAL RESULT

First the user has to register his RFID card along with his Gmail ID and password.

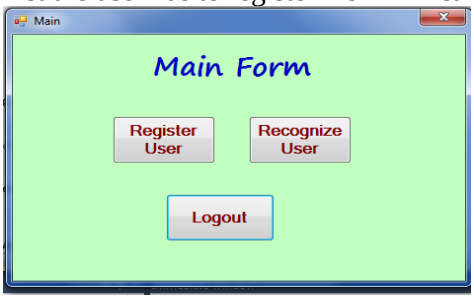

Figure.5. Main Form

Figure.6. Detect Face and Register

The user can register his face in the register user module and set a password. Once the user face is detected the system does image processing on the face and the stores it in the database.

Figure.7. Image Processing

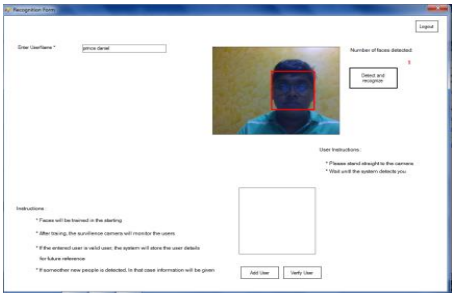

Figure.8. Recognition form

Then the user can verify his face in the recognition form for login purpose. The registered users can use the login page to get access to their data.

3. CONCLUSION

RFID and Fractal Recognition technologies are undoubtedly the core technologies of future security systems. At present, efforts are being made to integrate these two technologies on the same platform indifferent fields. Unlike conventional studies. This study proposed an implementation model of an RFID embedded with fractal recognition. Although it is quite representative, there are still exceptional situations, in which the proposed design would not work effectively. For example, if a specific type of event other than Object Event such as the registered user loses his RFID or makes emotions while recognition is done we may have to reconsider further optimizations like Every aspect of security in terms of data is discussed in this project but the user's perspective is not discussed. So, in the future enhancement, tracking the lost RFID will be included and even for the registered users specified time of access can be added.

REFERENCES

Fogla P, Sharif M, Perdisci R, Kolesnikov O and Lee W, Polymorphic blending attacks, in Proc. 15th Conf. on USENIX Security Symp. CA, USA, USENIX Association, 2006.

Johnson P, Tan B and Schuckers S, Multimodal fusion vulnerability to non-zero effort (spoof) imposters, in IEEE Int'l Workshop on Inf. Forensics and Security, 2010, 1-5.

Joy Winnie Wise D.C and Jeno Mactaline Pears J, Black Hole Attack Detection Using HLA with Optimized Link State Routing Protocol in Wanet, International Journal of Engineering and Computer Science, 5 (10), 2016, 18649-18654.

Lowd D and Meek, Good word attacks on statistical RFID filters, in 2nd Conf. on RFID and Anti-RFID, CA, USA, 2005.

Kavita, Manjeet Kaur, A Survey paper for Face Recognition Technologies, International Journal of Scientific and Research Publications, 6 (7), 2016 ,441.

Rodrigues R.N, Ling L.L and Govindaraju V, Robustness of multimodal biometric fusion methods against spoof attacks, J. Vis. Lang. Comput., 20 (3), 2009, 169–179.

Upendra C, Gopichand G, Survivability and Protection of Nodes and Links from Failures in WDM Mesh Networks, IJARCN ISR Journal, 1 (1), 2013.

Wei H, Shen L and Li X.H, Image Compression and Indexing Methods Based on Iterative Function System, J. Image and Graphics, 7 (11), 2002, 1198–1203.

Wittel G.L and Wu S.F, on attacking statistical RFID filters, in 1st Conf. on RFID and Anti-RFID, CA, USA, 2004.

Zeng W.Q, Wen W.Y and Sun W, Fractal Wavelet and Image Compression, Northeastern University Press, Shenyang, 2002.

Zhang J, He X, and Li J, Face Recognition Based on Geometrical Feature Points Extraction, J. Infrared and Laser Engineering, 28 (4), 1999, 40–43.