A Machine Learning Approach for Enhanced Fingerprint Recognition Technique

Heli Shah
B.Tech Biomedical Engineering
VIT University
Vellore, India

Rajat Arora
B.Tech Informational Technology
VIT University
Vellore, India

ABSTRACT

With the increasing awareness about the security systems, there has been a development of different types of biometric systems in this field. One of the most common and cost effective biometric systems is Fingerprint Biometrics. Enhanced Fingerprint Identification Technique describes mathematical algorithms to overcome the limitations faced while using the conventional fingerprint biometric systems. Enhanced Fingerprint Identification Technique provides improvised and efficient recognition process. Lumidigm sensor, captures images of skin at different wavelengths, has been used to get a multispectral image of fingerprint. GLCM algorithm is used for extracting features from the acquired fingerprint image. DTW Comparison is used for identification and verification process. Machine learning based amalgamated algorithms will overcome the hindrance faced in the recognition process while using the conventional fingerprint scanner.

Keywords

Fingerprint; GLCM algorithm; Dynamic Time Warping algorithm; fingerprint spoofing; biometric system

1. INTRODUCTION

In this 21st century, Humans prefer to live in a society which is completely secure. Security systems have applications in hospitals, defense, airports, R&D labs, and banks, industries such as mining, construction, and heavy manufacturing. They are generally used for access control and time-attendance needs. Security system consists of different types of biometric systems such as fingerprint biometrics, retinal biometrics, iris scanners, gait analysis biometrics, palm vein scanner etc. Biometric systems can be defined as an automated process to verify or recognize the identity of a person on the basis of physiological or behavioral characteristics. While much research has been done both to determine which traits can differentiate humans and to optimize that differentiation, the problem of determining if the presented trait originates from a living person has received relatively less attention. Between acquiring biometric data and delivering a result, there are various points where the overall security of a biometric access system can be compromised. Out of all these biometric scanners, fingerprint biometric is cost-effective and can be easily afforded by small firms. But the conventional fingerprint biometric scanners have limitations which hamper the recognition process at times. At times, people have difficulty in enrolling their fingerprint in the database. Such limitations have been targeted and overcome in this proposed enhanced fingerprint recognition technique.

2. LITERATURE REVIEW

2.1 Biometric Process

Firstly, raw biometric information of a person is acquired by the scanner which may have a camera, sensor or microphone. The camera may capture a face or iris, sensor may capture a fingerprint, and a microphone may capture a voice. The captured data is sent to feature extractor which is a software that extracts features, important and unique for determining the identity of a person. Minutiae points are extracted for fingerprint, distance between eyes may be calculated for face. The extracted features from the raw data are called templates, these templates are then sent to matcher, where the newly presented information is compared with the information already stored in the database. Further, it shows the output, whether the new input has access to the system or not.

2.2 Finger Skin Histology

The interface between a person and outside environment is done by human skin. The skin comprises of receptors for the nervous system, blood vessels to nourish cells, sweat glands for thermal regulation, sebaceous glands to aid oil secretion, hair follicles, etc. Skin is not a single layer but it is made of different layers. The superficial layer is epidermis, blood-bearing layer beneath epidermis is dermis, and subcutaneous skin layer, which contains fat and inert components.

The skin on the fingertip contains patterns such as ridges, valleys, and loops etc. which are commonly measured for fingerprint-based biometrics. Importantly, these patterns are just not found on the surface of the skin, they are also present below the superficial surface of the skin. For example, the border of the epidermal and dermal layers of skin is an undulating layer made of multiple protrusions of the dermis into the epidermis known as dermal papillae. These papillae follow the shape of the surface patterns and thus represent an internal fingerprint in the same form as the external pattern.

2.3 Types of Fingerprint Biometric System

There are three types of fingerprint biometric systems: Optical, Solid-state, and Ultrasound; each technology has strengths and weaknesses.

Optical fingerprint scanners capture data through total internal reflection (TIR). Raw data is generated by the differential reflectivity of friction ridges—which are in contact with a glass platen—and the valleys of the fingerprint (air). Illumination of the finger surface is done by one side of a prism and is reflected through the opposite side. Ridges and valleys are formed in contrast.

Solid-state sensors consist of an array of some kind of material that can measure physical characteristics of skin. The most common type of such array-based sensor is the capacitive sensor, having an array of capacitor plates. When a fingertip is kept on the sensing plate surface, ridges and valleys form opposite plate of a virtual capacitor. There will be air lodged between the sensing plate and skin, which will induce differential capacitance for valleys and ridges, thus creating an image. This raw image is acquired through the array. Thermal Sensors are also solid-state sensors. They sense the difference in temperature between the surface of ridges, which are in direct contact with the sensing surface, and valleys, whose radiated heat reaches the sensor via the medium of air. Piezoelectric sensors, nowadays used as solid-state sensors, generate images by calculating the variance in mechanical stress of ridges and valleys when a fingertip is kept on the sensing surface.

Ultrasound sensors have acoustic signals which are transmitted towards the fingertip surface. These acoustic waves travel at different speeds through ridges and air lodged under the skin. A receiver captures the reflected acoustic signal (echo). This receiver then generates a fingerprint image.

2.4 Fingerprint Sensor Attacks

The first attempt to weaken the security of fingerprint-based identification biometrics was done in 1920s when a person had used his experience in photography and engraving to forge concealed prints. A latent fingerprint was dusted to disclose and increase contrast, and a photograph was taken. The negative was used to etch the print onto a copper plate. Lightly greased, the plate could be used to leave counterfeit latent prints on objects.

In the recent times, artificial fingers made from soft material could be falsely accepted as real fingers on widely available biometric fingerprint sensors. Due to this, development of research area to prevent this types of attacks have been started.

When the goal of the spoof is to gain access that another person has, the first step is to retrieve the fingerprint of that person—i.e., a person that is already enrolled and whose data is already there in the database. There are two approaches for acquiring an enrolled subject’s fingerprint: cooperative retrieval and non-cooperative retrieval. In cooperative retrieval, the subject allows the collection of one or more fingerprints. The fingerprint is usually collected by pressing the finger in a small amount of suitable material such as wax or dental mold material; the impression creates a mold from which artificial fingers can be cast. A variety of materials has been used for casting such as silicone, rubber, tape, moldable plastic, plaster, clay, and dental molding material. In a real-world scenario, it is highly unlikely that a person would agree to produce a mold from a finger. Printed circuit board etching is a successful molding technique used for non-cooperative retrieval which produces “gummy” and other soft material artificial fingers

3. LIMITATIONS OF CONVENTIONAL FINGERPRINT SCANNER

Conventional fingerprint scanner only scans the superficial layer of the skin, thus it may be susceptible to error. Many scanning systems could be cheated by employing artificial fingers or perhaps showing another person's finger. False Acceptance Rate and False Rejection Rate is not nil. Fingerprint spoofing can be easily done by imprinting fingerprint on a gelatin, silicon or rubber surface.

Sometimes it may take many swipes of the fingerprint to register. Fingerprints of people working in chemical sectors, laborers working in industrial sector have difficulty in registering their fingerprint due to presence of dirt, dust, moisture on their skin. Cuts, marks or wrinkles can also hamper the identification procedure. Moisture, dirt, and dust on the sensing surface can also lead to false match.

4. METHODOLOGY

To overcome the limitations related to conventional fingerprint biometric system, Enhanced Fingerprint Recognition Technique makes use of multispectral sensors in order to capture information-rich data about the surface and subsurface features of the skin of the finger. Lumidigm sensor was used to collects multiple images of the finger under a variety of optical conditions. The raw images are captured using different wavelengths of illumination light, different polarization conditions, and different illumination orientations. In this way, each of the raw images, acquired from this sensor, contains somewhat different and complementary information about the finger. The different wavelengths (frequencies) penetrate the skin to different depths and are absorbed differently by various chemical components of the skin. Finally, these images acquired at different frequencies are merged and the resultant image is further used for further processing.

The raw image is read on Matlab. GLCM method is used to extract features from the training data set. Dynamic Time Warping comparison method is used for comparing the features of test dataset with trained dataset.

Machine learning algorithm is capable of learning is sparse, high-dimensional spaces with very few training examples. This approach has two main benefits: It can tolerate the presence of ambiguous fingerprint images in the training set, and it can effectively identify the most difficult fingerprint images, at times containing noise, in the test set. By accepting these images the accuracy of the system improves significantly.

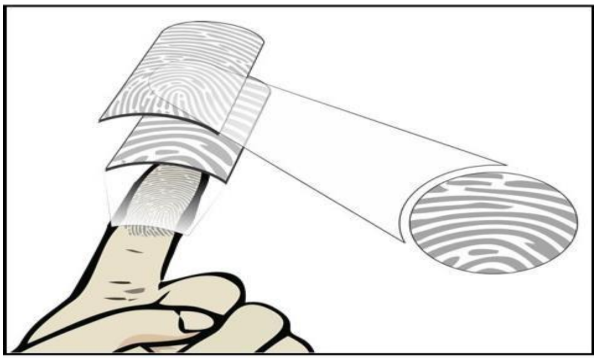


Fig 1: Image acquisition through multispectral technique

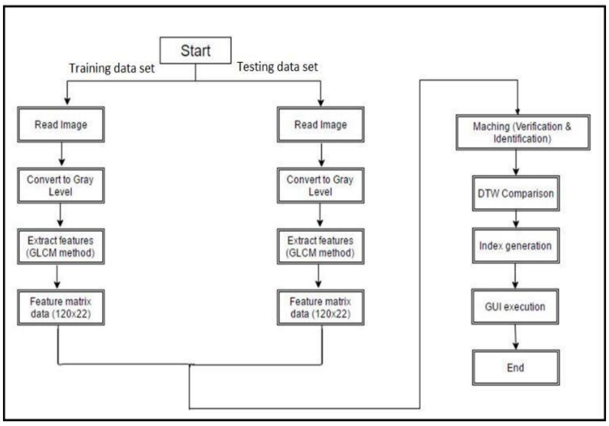

Start
Training data set
Testing data set
Read Image
Convert to Gray Level
Extract features (GLCM method)
Feature matrix data (120x22)
Read Image
Convert to Gray Level
Extract features (GLCM method)
Feature matrix data (120x22)
Maching (Verification & Identification)
DTW Comparison
Index generation
GUI execution
End

Fig 2: Flow chart of Enhance Fingerprint Recognition Technique

Gray level co-occurrence matrix (GLCM) is used to extract second order statistical texture features of an image such as Angular Second Moment, Correlation, Inverse Difference Moment, and Entropy, Homogeneity, Variance etc. These texture features have high discrimination accuracy, requires less computation time and hence provides better results than localization algorithm. Dynamic time warping (DTW) which is a much more robust algorithm to measure parameters of time series as it allows equivalent shapes to match even if they are out of phase on the time axis. Because of this flexibility, verification and identification procedure has been carried out using this method.

A database of 120 images was taken for training. 22 features through GLCM method were extracted from each image. An excel sheet is made of the trained data set (22x120) having a numeric data of extracted features for 120 images. This excel sheet is converted into a .mat file and then loaded in Matlab. While carrying out a recognition process, the user's fingerprint will be captured through multispectral sensor, 22 features will be extracted from the raw image. These extracted features are test dataset. Each data of test data set is compared with the trained data set through DTW comparison method. The trained data set having the least error value with the test data set is the recognized as the correct match.

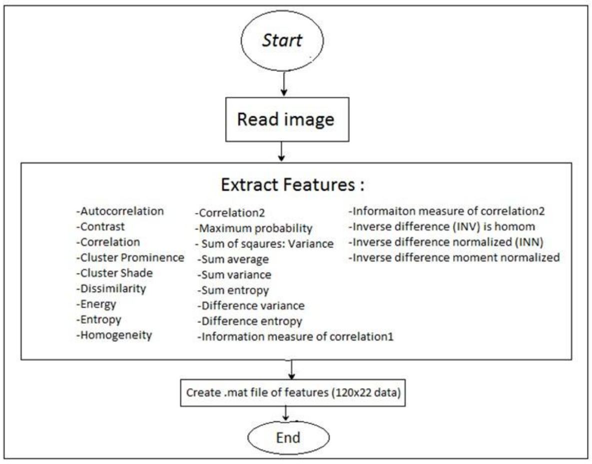


Fig. 3. Flow chart for Feature Extraction

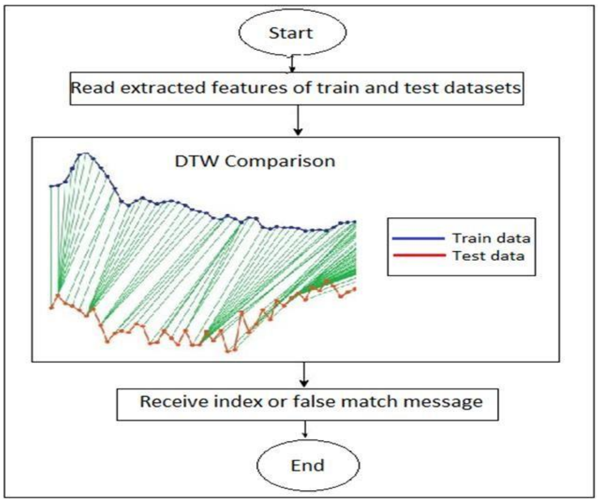

Start
Read extracted features of train and test datasets
DTW Comparison
Train data
Test data
Receive index or false match message
End

Fig 4. Flow chart of DTW Comparison

4.1 Advantages

Multispectral technology will prevent the spoofing attacks. Fingerprint spoofing is done by imprinting fingerprint on a rubber or silicone surface. Conventional fingerprint scanners couldn't differentiate between real- fingerprint layer or spoofed layer, but multispectral technology based sensors, capable of capturing multiple layers, will be able to differentiate between skin layers and spoofed surface.

As data is captured at different frequencies, there won't be any problem is capturing data from a finger which is having moisture, dirt, cut, or dust on its surface.

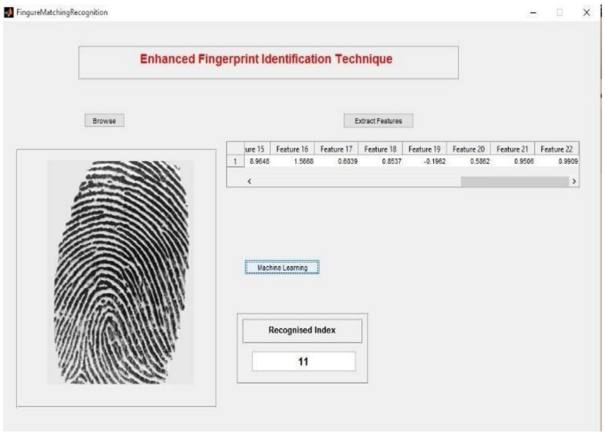
Recognition process can be carried out easily for the elderly people having wrinkles, patients having injuries and industrial workers.

Due to the Machine learning based algorithm, false acceptance rate and false rejection rate will decrease significantly.

5. OUTCOME

Feature extraction code and machine learning code for recognition process have been developed in Matlab. Graphic User Interface (GUI) format in Matlab is used for executing the successful working of the code. A trained database has 120 images from 15 users. Each user had to scan their finger in various positions. Users have been given user id starting from 1 to 15. Apart from this 120 images, 5 images have been taken for testing purpose. These five images comprise of different types.

The first image for testing is of user having User ID 11. Figure 5 shows the GUI execution, the test image is loaded in Matlab, then feature extraction is done and lastly, through DTW comparison, the correct index is recognized.


FingureMatchingRecognition

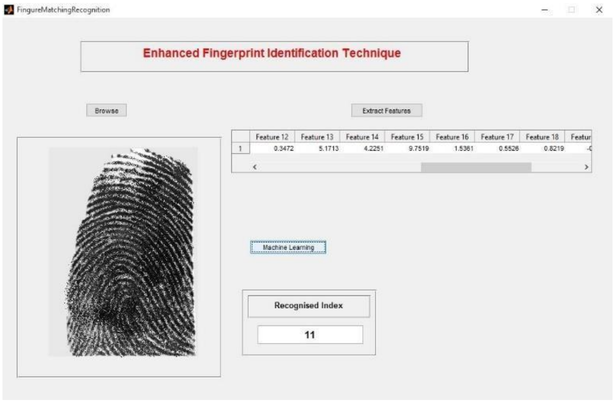
Enhanced Fingerprint Identification Technique

	ure 15	Feature 16	Feature 17	Feature 18	Feature 19	Feature 20	Feature 21	Feature 22
1	8.9648	1.5668	0.6039	0.8537	-0.1962	0.5862	0.9506	0.9909

Recognised Index
11

Fig. 5. GUI execution of test image which is in database

The second image for testing is of user having User ID 11, but this image was acquired when the user had dirt and dust on the surface of the skin. Figure 6 shows the GUI execution, the test image is loaded in Matlab, then feature extraction is done of the image having noise and lastly, even though the image was not so proper, through DTW comparison the correct index is recognized.


FingureMatchingRecognition
Enhanced Fingerprint Identification Technique
Browse
Extract Features
Machine Learning

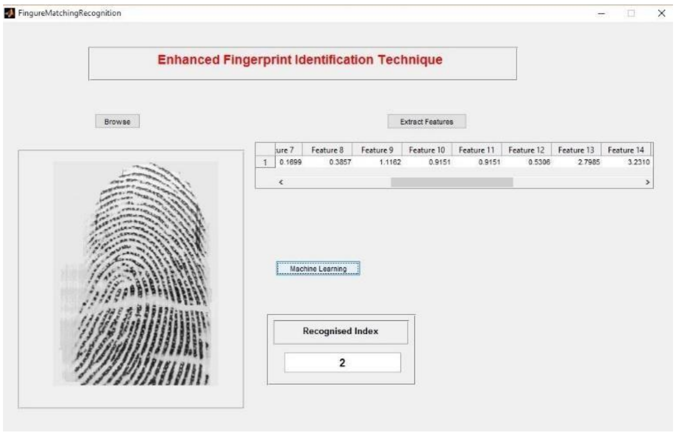
	Feature 12	Feature 13	Feature 14	Feature 15	Feature 16	Feature 17	Feature 18	Featur
1	0.3472	5.1713	4.2251	9.7519	1.5361	0.5526	0.8219	-0

Recognised Index

11

Fig. 6. GUI execution of test image acquired from a surface having dirt

The third image for testing is of user having User ID 2, but this image was acquired when the user had a cut on the surface of the skin. Figure 7 shows the GUI execution, the test image is loaded in Matlab, then feature extraction is done of the image having disruption of minutiae and lastly through DTW comparison the correct index is recognized.


FingureMatchingRecognition
Enhanced Fingerprint Identification Technique
Browse
Extract Features
Machine Learning

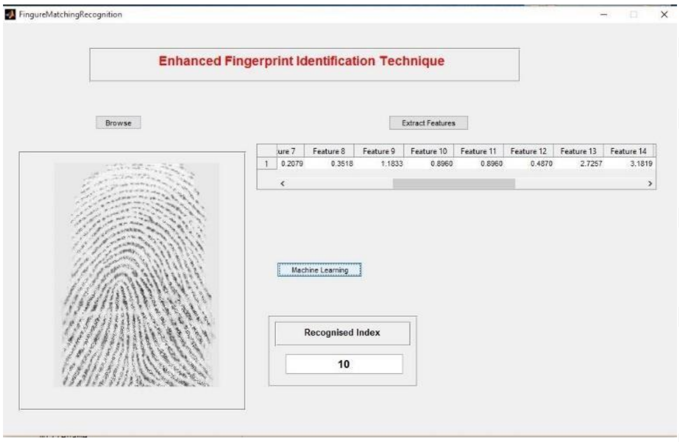
	ure 7	Feature 8	Feature 9	Feature 10	Feature 11	Feature 12	Feature 13	Feature 14
1	0.1699	0.3857	1.1162	0.9151	0.9151	0.5306	2.7985	3.2310

Recognised Index

2

Fig. 7. GUI execution of test image acquired from a cut-surfaced skin

The fourth image for testing is from the user having moisture in the skin layers and having User ID 10. Figure 8 shows the GUI execution, the test image is loaded in Matlab, then feature extraction is done of the image having interference and lastly through DTW comparison the correct index is recognized.


FingureMatchingRecognition
Enhanced Fingerprint Identification Technique
Browse
Extract Features
Machine Learning

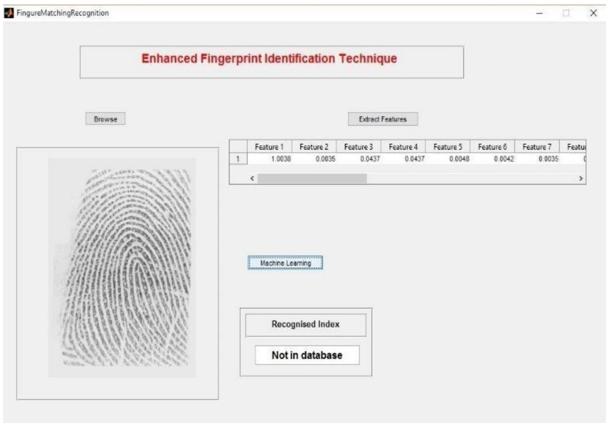
	ure 7	Feature 8	Feature 9	Feature 10	Feature 11	Feature 12	Feature 13	Feature 14
1	0.2079	0.3518	1.1833	0.8960	0.8960	0.4870	2.7257	3.1819

Recognised Index

10

Fig. 8. GUI execution of test image acquired from a moisture surfaced skin

The fifth image for testing is from an unknown user whose data is not enrolled in the trained database. Figure 9 shows the GUI execution, the test image is loaded in Matlab, then feature extraction is done and lastly through DTW comparison the user is rejected as his data is not recognized by anyone from the database.


FingureMatchingRecognition
Enhanced Fingerprint Identification Technique
Browse
Extract Features
Machine Learning

	Feature 1	Feature 2	Feature 3	Feature 4	Feature 5	Feature 6	Feature 7	Featu
1	1.0038	0.0035	0.0437	0.0437	0.0048	0.0042	0.0035	0

Recognised Index

Not in database

Fig 9: GUI execution of test image of an unknown user, not in the database

6. CONCLUSION

Therefore, by verifying the test dataset of images having dirt, dust, moisture on the surface of the skin it can be concluded that the amalgamated algorithm can carry the process of identification and verification in spite of having interference in the raw image. This method proves its robustness in finding the false match and preventing spoofing. Moreover, from the the coding perspective of comparison between train data set and test data set, it is done diligently using machine learning approach which has decreased the FAR and FRR significantly.

This machine learning based algorithm holds humongous future scope and can be widely used and implemented in variety of applications.It can be combined with mobile phones to improve the Fingerprint scanner technology and make the use of it more efficient. For example, many users tend to use their cell phones in situations when their hands have some sweat or dirt present. In that case this algorithm can help improve the recognition. Similar technique can also be incorporated where there is a need to record or partially damaged fingerprints from an object or place. For example taking the distorted fingerprints from a crime scene or theft scene are usually difficult to analyze but using this technique it can be done exactly.

7. REFERENCES

[1] J.D.Woodward,N.M.Orlans,andP.T.Higgins,Biometrics,New York: McGraw-Hill, 2002.

[2] S. Prabhakar, S. Pankanti, A. K. Jain, "Biometric Recognition: Security and Privacy Concerns", IEEE Security & Privacy, March/April 2003, pp.33-42.

[3] SharathPankanti, "On the Individuality of Fingerprints", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 24, No.8, August 2002.

[4] US-VISIT Program Overview, Department of Homeland Security. (2004, Dec.13).[Online].Available:http://www.dhs.gov/dhspublic/interapp/edito rial/editorial_0445.xml

[5] Undergraduate Curriculums (2014, Dec. 13). [Online]. Available:http://www.lcsee.cemr.wvu.edu/ugrad/curriculum

[6] Course Catalog (2004, Dec. 13). [Online]. Available: http://www.cse. nd.edu/academics/catalog.php

[7] IndustrialTechnology(2015,Dec.13).[Online].Available:http ://www. tech.purdue.edu/it/resources/biometrics/it-345.html/

[8] Sweta, Amit Walia, "Classification and Improvement of Fingerprint Verification Using Support Vector Machine" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 6, ISSN: 2277 128X June 2014

[9] Rupinder Saini, Narinder Rana "Comparison of Various Biometric Methods" International Journal of Advances in Science and Technology (IJAST) Vol 2 Issue I (March 2014) ISSN 2348-5426

[10] Urvik Patel, “A Study on Fingerprint (biometrics) Recognition” International Journal of Engineering and Sciences (eISSN-2394-6180), Volume -1 Isuue-2, Feb-2015

[11] Antonio Iula, Alessandro Savoia, Giosue Caliano, “ Capacitive micro- fabricated ultrasonic transducers for biometric applications” Microelectronic Engineering 88 (20122) 2278-2280

[12] A. Krizhevsky, I. Sutskever, G. Hinton, Adv. Neural Inf. Process. Syst.25, 1097–1105, 2015.

[13] Annett, M., Grossman, T., Wigdor, D., and Fitzmaurice, G. Medusa: A Proximity-Aware Multi-touch Tabletop. Proc. UIST 2011, pp.337–382

[14] H. B. Kekre, Tanuja K. Sarode, “Fast Codebook Generation Algorithm for Color Images using Vector Quantization,” Int. Journal of Computer Science and Info. Technology, Vol. 1, No. 1, pp.: 7-12, Jan

[15] Qiu, “Color Image Indexing Using BTC”, IEEE Transactions on Image Processing, Volume 12, Number 1, pp.93-101, Jan 2013

[16] H. Schulz-Mirbach, “Constructing invariant features by averaging techniques”, In IAPR International Conference on Pattern Recognition (ICPR), Volume 2, pp 387–390, Jerusalem, Israel, October 1994.

[17] Tappert, C. & Das, S. Memory and time improvements in a dynamic programming algorithm for matching speech patterns. IEEE Trans. Acoustics, Speech, and Signal Proc., Vol. ASSP-26, 583-586.

[18] Agrawal R, Lin KI, Sawhney HS, Shim K Fast similarity search in the presence of noise, scaling, and translation in times-series databases. In: Proceedings of the 21st international conference on very large databases, pp 490–501, Jan 2010