iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL
FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** V **Month of publication:** May 2018

DOI: http://doi.org/10.22214/ijraset.2018.5341

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue V, May 2018- Available at www.ijraset.com

A Study of Covert Surveillance in Multimodal Biometrics

Nuthakki Praveena[1], Dr. Ashish B. Sasankar[2], Chilakalapudi Meher Babu[3]
[1]Assistant Professor, Information Technology, V.R.Siddartha Engg College. Vijayawada, A.P., India
[2]Professor, Head,Dept of MCA, G.H.Raisoni Institute of It, Hariganga Campus, Midc,Nagpur-India,
[3]Ph.D. Research Scholar, Post-Graduate Teaching Department of Electronics & Computer Science Dept, R.T.M. Nagpur University, Nagpur – India,

Abstract: Current world is facing threats from terrorism and it has become a global concern to implement strict security and surveillance measures. The biometric systems have become good option for identity of a person based on the physical or behavioral quality of the individual such as fingerprints, palm print, face, voice, iris etc., such as secure access control, law enforcement etc., Thus, these systems may be viewed as pattern recognition engines that can be incorporated in every part of human body is unique and if we can consistently capture the specified area or trait, efficient biometric authentication system can be form different variants are used for implementation of biometric authentication systems.

Keywords: Fingerprint Recognition, Pattern recognition, Wavelet, Texture, orientation angle.

I. INTRODUCTION

Security concerns are the major concern in today's world and are continuing to grow in intensity and complexity. Security is an aspect that is given top priority by organizations, educational institutions, political and government in identity and fraud issues. In response to the new threats, organizations need to implement or update a personnel security program to prevent unauthorized access to control systems and critical information.

Technologies called biometrics can automate the identification of people by one or more of their distinct physical or behavioural characteristics. They are pattern recognition systems, which make a personal identification by determining the authenticity of the specific characteristic possessed by the user. Biometrics has come to parameters like iris, voice, fingerprints, face characteristics important role in fingerprints have been one of the most widely used and accepted biometric.

The fingerprint properties of a person are very accurate and are unique to an individual. Authentication systems based on fingerprint have proved to produce low false acceptance rate and false rejection rate, along with other advantages like easy and low cost implementation procedure.

II. BIOMETRIC TECHNOLOGY

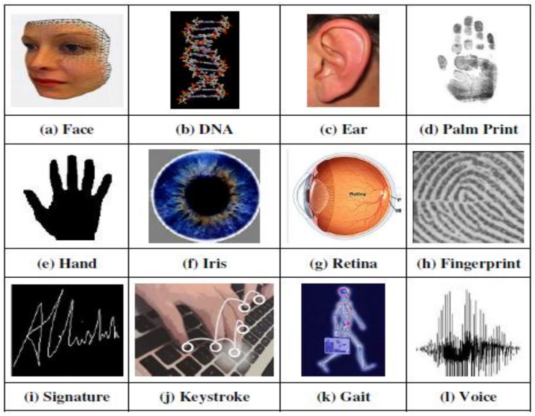
Biometric identification systems are essentially pattern recognition systems. They use acquisition devices such as cameras and scanning devices to capture images, recordings or measurements of an individual's characteristics and computer hardware and software to extract, encode, store and compare these characteristics. As the process is automated, biometric decision-making is generally very fast, and in most cases, takes only a few seconds in real time.

There are two modes in which biometric systems can be used. They are verification and identification. 'Verification', also called 'authentication', 'Identification' is used to establish a person's identity, that is, to determine who a person is. Although biometric technologies measure different characteristics in substantially different ways, all biometric systems involve similar processes that can be divided into two distinct stages:

A. Enrolment and
B. Verification or Identification.

In enrolment, a biometric system is trained to identify a specific person. The person first provides an identifier, such as an identity card. The biometric is linked with the identity specified on the identification document. He or she then presents the biometric (e.g., fingerprint or iris) to an acquisition device.

Types of Biometric technologies


(a) Face (b) DNA (c) Ear (d) Palm Print
(e) Hand (f) Iris (g) Retina (h) Fingerprint
(i) Signature (j) Keystroke (k) Gait (l) Voice

C. Physiological Biometric Traits

These are based on physical characteristics of human body. Fingerprint, palm print, hand vein, hand/finger geometry, iris, retina, face, ear, odor or the DNA information of an individual come in this category.

D. Fingerprints

A fingerprint looks at the patterns found on a fingertip. There are a variety of approaches to fingerprint verification. Some emulate the traditional police method of matching minutiae; others use straight pattern-matching devices; and still others are a bit more unique, including things like moiré fringe patterns and ultrasonic. Some verification approaches can detect when a live finger is presented; some cannot shows location of fingerprints on human hand and a typical fingerprint captured through optical fingerprint scanner.

A greater variety of fingerprint scanning devices are available than for any other biometric some of them these devices and processing costs fall, using fingerprints for user verification is gaining acceptance despite the common-criminal stigma. It is not surprising that the workstation access application area seems to be based almost exclusively on fingerprints, due to the relatively low cost, small size, and ease of integration of fingerprint authentication devices.

E. Hand Geometry

Hand geometry involves analyzing and measuring the shape of the hand. This biometric offer a good balances of performance characteristics and is relatively easy to use. It might be suitable where there are more users or where users access the system infrequently and are perhaps less disciplined in their approach to the system.

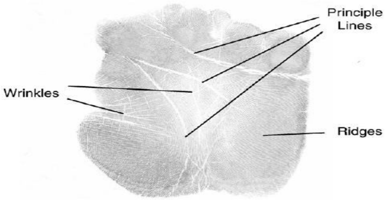
F. Hand Vein Geometry

A person's veins are completely unique. Twins don't have identical veins, and a person's veins differ between their left and right sides. Many veins are not visible through the skin, making them extremely difficult to counterfeit or tamper with. Their shape also changes very little as a person ages

To use a vein recognition system, you simply place your finger, wrist, palm or the back of your hand on or near the scanner. A camera takes a digital picture using near-infrared light. The haemoglobin in your blood absorbs the light, so veins appear black in the picture. As with all the other biometric types, the software creates a reference template based on the shape and location of the vein structure. This template can be used for matching purpose.

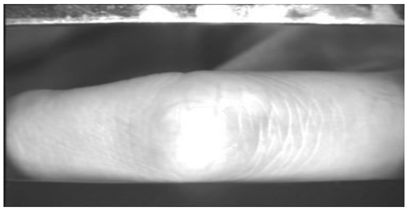
G.   Palm prints

The palms of the human hands contain pattern of ridges and valleys much like the fingerprints. The area of the palm is much larger than the area of a finger and, as a result, palm prints are expected to be even more distinctive than the fingerprints. Since palm print scanners need to capture a large area, they are bulkier and more expensive than the fingerprint sensors. Human palms also contain additional distinctive features such as principal lines and wrinkles that can be captured even with a lower resolution scanner, which would be cheaper. Finally, when using a high-resolution palm print scanner, all the features of the palm such as hand geometry, ridge and valley features, principal lines, and wrinkles may be combined to build a highly accurate biometric system.



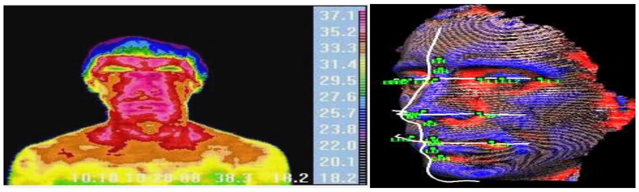
H. Finger-knuckle Print

Finger-knuckle print (FKP) refers to the image pattern of the outer surface around the phalange joint of one’s finger, which is formed by bending slightly the finger-knuckle. FKP contains rich texture information formed by wrinkles present on finger back surface.



I. Face

Face recognition analyzes facial characteristics. It requires a digital camera to develop a facial image of the user for authentication. Because facial scanning needs an extra peripheral not customarily included with basic PCs, it is more of a niche market for network authentication. With security cameras presents in variety of public places facial recognition is a viable option for biometric identification.



J. Iris

An iris-based biometric, on the other hand, involves analyzing features found in the colored ring of tissue that surrounds the pupil.

(A) (B) (C) (D)

(a) Iris Capturing devices (b) Handheld Iris Scanner (c) Captured iris Image (d)

K. Behavioural Biometric Traits

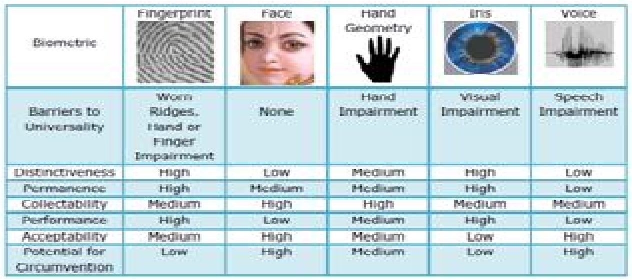
The behavioural biometrics deals with the way certain act is performed by human. This includes speaking, writing, walking etc. We discuss here few important behavioural biometric traits. Human handwriting style is unique from person to person. At first glance, using handwriting to identify people might not seem like a good idea. After all, many people can learn to copy other people's handwriting with a little time and practice. It seems like it would be easy to get a copy of someone's signature or the required password and learn to forge it. But biometric systems don't just look at how you shape each letter; they analyze the act of writing.

(a) Dynamic Signature Capturing Devices (b) Dynamic Signature showing Different

L. Keystroke Dynamics

The keystroke dynamics are captured entirely by software, so the technique can be applied to any system that accepts and processes keyboard input events. Keystroke dynamics can be used for single authentication events or for continuous monitoring.

Comparison of Key Biometric Technologies



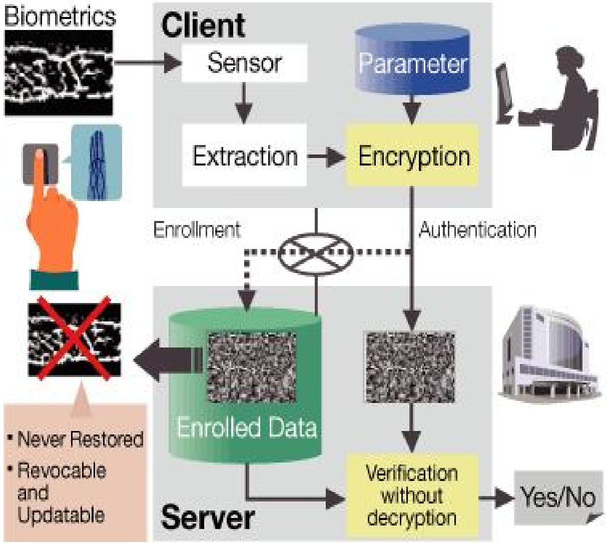
Biometric	Fingerprint	Face	Hand Geometry	Iris	Voice
Barriers to Universality	Worn Ridges, Hand or Finger Impairment	None	Hand Impairment	Visual Impairment	Speech Impairment
Distinctiveness	High	Low	Medium	High	Low
Permanence	High	Medium	Medium	High	Low
Collectability	Medium	High	High	Medium	Medium
Performance	High	Low	Medium	High	Low
Acceptability	Medium	High	Medium	Low	High
Potential for Circumvention	Low	High	Medium	Low	High

III.BIOMETRIC SYSTEM ARCHITECTURE

A. Biometric System can Operate In the Following Two Modes

1)Verification (Matching): A one to one comparison of a captured biometric with a stored template to verify that the individual is who he claims to be. This can be achieved in conjunction with a smart card, username or ID number.

2)Identification (Recognition): A one to many comparisons of the captured biometric against a biometric database in attempt to identify an unknown individual. The identification only succeeds in identifying the individual if the comparison of the biometric sample to a template in the database falls within a previously set threshold. The first time an individual uses a biometric system is called an enrolment. During the enrolment, biometric information from an individual is stored. In subsequent uses, biometric information is detected and compared with the information stored at the time of enrolment.



IV.FALSE ACCEPT RATE OR FALSE MATCH RATE (FAR OR FMR)

The probability that the system incorrectly matches the input pattern to a non-matching template in the database. It measures the percent of invalid inputs which are incorrectly accepted.

A. False Reject Rate or False Non-Match Rate (FRR or FNMR)

The probability that the system fails to detect a match between the input pattern and a matching template in the database. It measures the percent of valid inputs which are incorrectly rejected.

B. Receiver Operating Characteristic or Relative Operating Characteristic (ROC)

The ROC plot is a visual characterization of the trade-off between the FAR and the FRR. In general, the matching algorithm performs a decision based on a threshold which determines how close to a template the input needs to be for it to be considered a match. If the threshold is reduced, there will be less false non-matches but more false accepts. Correspondingly, a higher threshold will reduce the FAR but increase the FRR.

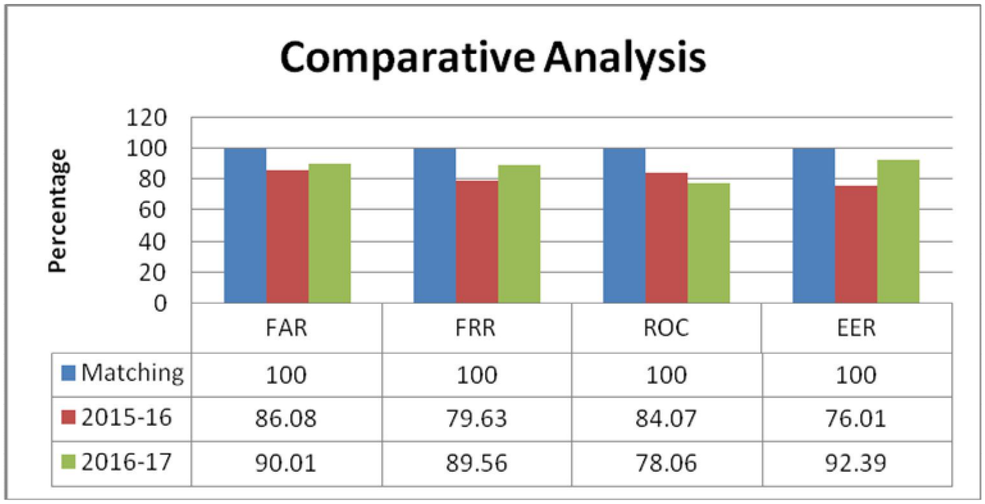
C. Equal Error Rate or Crossover Error Rate (EER or CER)

The rate at which both accept and reject errors are equal. The value of the EER can be easily obtained from the ROC curve. The EER is a quick way to compare the accuracy of devices with different ROC curves. In general, the device with the lowest EER is most accurate. Obtained from the ROC plot by taking the point where FAR and FRR have the same value.

Other metrics which are related to the sensor devices are Failure to Enroll Rate (FTE), Failure to Capture Rate (FTC) & Template Capacity.

As FAR and FRR are interdependent, it is more meaningful to plot them against each other, Each point on the plot represents a hypothetical system’s performance at various sensitivity settings. With such a plot, you can compare these rates to determine the crossover error rate (Equal Error Rate). Lower the CER (EER), more accurate the system.

	FAR	FRR	ROC	EER
Matching	100	100	100	100
2015-16	86.08	79.63	84.07	76.01
2016-17	90.01	89.56	78.06	92.39



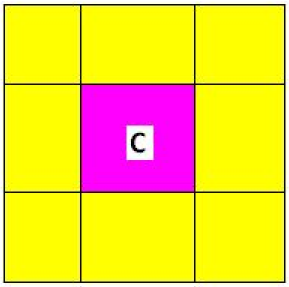
D. Pre-processing & Template Generation

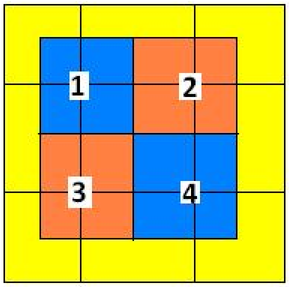
In order to match the fingerprints we need to form Representation (Template) of fingerprint image. This is a machine readable representation completely captures the invariant and discriminatory information in a fingerprint image. We divide the input image in non overlapping sectors of size W*W pixels. Normalization [36] is done to remove the effects of sensor noise and finger pressure differences. Let I(x, y) denote the gray value at pixel (x, y), Mi and Vi, the estimated mean and variance of sector Si, respectively, and Ni(x, y), the normalized gray-level value at pixel (x, y). For all the pixels in sector Si, the normalized image is defined as:

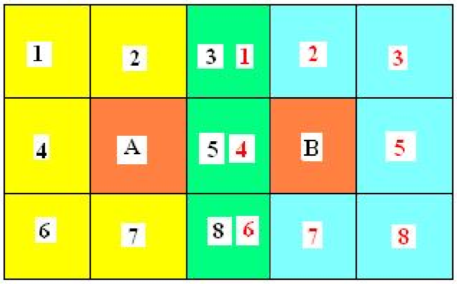
$$N_i(x,y) = M_0 + \sqrt{\frac{V_0 * (I(x,y) - M_i)^2}{V_i}} \quad \text{If } I(x,y) > M_i$$

$$N_i(x,y) = M_0 - \sqrt{\frac{V_0 * (I(x,y) - M_i)^2}{V_i}}$$

\Structure tensor based Orientation estimation algorithm have proposed a modified technique based on gradient calculation which exploits the fact that the orientation field tend to be continuous in the neighboring regions. According to orientation of central point based on the orientation of neighboring blocks at four corners and their field strength (also called as coherence). Here use an averaging filter to the continuous vector filed calculated from the local gradient angle. Both the approaches give reasonably good approximation of the orientation field. (a) shows such a scenario calculate the orientation of block 'C', continuous vector field of neighboring 5*5 blocks is considered and averaged. Blocks 1,2,3,4 are used to estimate the orientation of center block 'C'.







IV. CONCLUSION

A. *Proposed Core Point Detection Algorithm*

Considering all above discussed features, we propose a formal algorithm which combines them to estimate the core point location. The core point detection mechanism proposed works in two main stages.

1) Detect possible core point (Singularity) region. We mainly consider Finger core but the mask used gives presence of Arch in the form of high curvature ridges also.

2) Detect a single point in the region by weighted sum of features discussed above. This step decides presence of core point as a center of a 16X16 Pixels window. The algorithm for core point detection is given as follows:

3) Read the fingerprint Image

4) Preprocess & Segment the fingerprint image to remove errors due to non-uniform pressure and illumination while scanning of the fingerprint.

5) Estimate the orientation field by optimized neighbourhood averaging.

6) Calculate the Gradient Field Coherence, Poincare index, Angular Coherence features & normalize these feature vectors to a 0 to 1 range.

7) Calculate loop field Strength at each point in the orientation field, using the developed orientation field mask

8) Normalize the loop field strength array in a range of 0 to 1.

9) Threshold the loop field strength array to locate the core point, this threshold for our method ranges in the order of (.34 to .45). Take the centroid of the region if it consists more than one block.

10) If more than one core points regions are located then take the region towards upper end or take centroid.

11) Separate 5X5 block size (Each block of size 16X 16 Pixels considered here) area of the Fingerprint & its corresponding parameters.

12) Using These Parameters determine the exact core point location by weighted sum as discussed below.

13) We copy the region into a 5X5 size array and evaluate above discussed features for the regions. Final core point is decided by weighted sum of the above parameters for core point thecoherence & cosine component sum should be minimum and Poincare index should be maximum, hence we find final region weighted sum as

Core[x, y] = Coherence[x, y] + Angular Coherence [x, y] -Poincare[x, y] (3.30)

The current era is driven by technology and now it is possible to have compact biometric scanners of various types and the computers that can handle enormous data and calculations required for biometric authentications are now available at affordable cost. Besides this current world is facing threats from terrorism and it has become a global concern to implement strict security and surveillance measures. The biometric systems have become good option for access control, human identification and authorization because of their advantages over conventional security systems.

REFERENCES

[1] A.K. Jain, R. Bolle and S. Pankanti, Biometrics: Personal Identification in a Networked Society, Kluwer Academic Publishers, 1999

[2] D. Polemi, "Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, Including an Appraisal of the Areas Where They are Most Applicable," Final Report, April 1997.

[3] A. K. Jain and A. Ross, “Learning User Specific Parameters In A Multibiometric System”, Proc. Int. Conf. Image Processing (ICIP), New York , pp. 57-60, 2002

[4] K. Nandakumar, Y. Chen and A. K. Jain, “Quality Based Score Level Fusion In Multibiometric Systems”, Proc. 18th Int. Conf. Pattern Recognition (ICPR), pp. 473-476, 2006

[5] J.Berry and D.A.Stoney, “ The history and development of finger printing in advances in fingerprint technology”, CRC Press, Florida, 2nd Edition, pp. 1-40, 2001

[6] Emma Newham, “The Biometric report”, SJB services, 1995

[7] Federal Bureau of Investigation, “The Science of Fingerprints: Classification and Uses”, US Government Printing office, Washington D.C., 1984

[8] A.K.Jain, S.Prabhakar, L.Hong and S.Pankanti, “Filter based Fingerprint Matching”, IEEE Transactions on Image Processing, Vol.9, No. 5, pp. 846-859, May 2000

[9] W. Yongxu, A. Xinyu, D. Yuanfeng and Y. Li, “A Fingerprint Recognition Algorithm Based on Principal Component Analysis” ,Proceedings of IEEE Region 10 Conference TENCON, pp.14-17,2006.

[10] ASME B46.1, Surface texture: Surface roughness, waviness and lay,1995

[11] Yuanyan Tang, “Status of Pattern Recognition with Wavelet Analysis” Front. Comput. Sci. China, pp.268-294, 2008

[12] T. Merryman, K. Williams, G. Srinivasa, A. Chebira, and J.Kovacevic, “A multiresolution enhancement to generic classifiers of subcellular protein location images,” Proc. in IEEE Int. Symp. Biomed. Imaging, Arlington, VA, pp.570–573, Apr. 2006

[13] A. Chebira, T. Merryman, G. Srinivasa, Y. Barbotin, C. Jackson,R. F. Murphy, and J. Kovacevic, “A multiresolution approachto automated classification of subcellular protein location images”, BMC Bioinformatics, 2007.

[14] Jian-De Zheng, Yuan Gao and Ming-Zhi Zhang, “Fingerprint Matching Algorithm Based on Similar Vector Triangle,” Second International Congress on Image and Signal Processing, pp.1-6, 2009.

[15] Shubhangi Vaikole, S.D.Sawarkar, Shila Hivrale,Taruna Sharma, “Minutiae Eetracion from Fingerprint Images”, IEEE International Advance Computing Conference, pp. 691-696, 2009.

[16] Ishmael S. Msiza, Brain Leke-Betechuoh, Fulufhelo V. Nelwamondo and Ntsika Msimang, “A Fingerprint Pattern Classification Approach Based on the Coordinate Geometry of Singularities”, Proceedings of the 29 IEEE International Conference on Systems, Man, and Cybernetics, pp. 516-523, 2009.

AUTHOR PROFILE

Chilakalapudi Meher Babu did his M.Tech in Computer Science and Engineering from JawaharlalNehru Technological University, Kakinada, Andhra Pradesh (INDIA) and pursuing Ph.D in R.T.M. Nagpur University, Nagpur(India) , Currently pursuing Ph.D in the Post-Graduate Teaching Department of Electronics & Computer Science Dept, R.T.M. Nagpur University, Nagpur, India.He has 16 National and International Journal Publications to his credit. His area of interest in research includes MANET, Network Intrusion Detection System on Wireless Lan’s, IP Address, Routing Algorithms etc.,

Dr. Ashish B.Sasankar did his MCA. M.Tech (CSE), M.Phil. (Computer Science) & Ph.D. in Computer Science from R.T.M. Nagpur University (India). He has a rich experience of 16 years in the field of Education. Currently, he is the Head of the Department of MCA in the most prestigious G.H.Raisoni Institute of information Technology [GHRIIT], Nagpur [India]. He is a Ph.D Guide for Computer Science in the Faculty of Science in R.T.M. Nagpur University, Nagpur (India) and guiding many of his research scholars doing their Ph.Ds in Computer Science in R.T.M.Nagpur University, Nagpur. He has 40 National & International Journal Publications to his credit. He is a Member of the IEEE and CSI.

Nutakki Praveena did her M.Tech in Information and Technology from JNTU- Vizianagaram University, Visakhapatnam. A.P. INDIA. Her area of expertise includes Computer Networks, wireless LANs, IP address, routing algorithms, Information Technology. She is working as Assistant Professor in department of information Technology at V.R.SIDDARTHA OF ENGINEERING College, Vijayawada, and Andhra Pradesh, India.