iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** II **Month of publication:** February 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 3 Issue II, February 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Enhancing Biometric System with Wavelet Quantization Based Watermarking

Kamod Renuka R., Khalkar Sonali B., Mahajan Roshani R., Sonparote Neha V.

student of computer Department, PVG's college of engg.Nashik
& Savitri Bai Phule Pune University
India

***Abstract*— As Malicious attacks greatly threaten the security and reliability of biometric systems, ensuring the authenticity of biometric data is becoming increasingly essential. In this paper we perform a watermarking based two-stage authentication framework to address this problem. During data collection, face features are embedded into fingerprint image of the same individual as data credibility token and secondary data authentication source. At the first phase of authentication, the credibility of input data is defined by checking the validness of extracted template. Due to the specific features of face watermarks, the face detection-based categorization strategies are introduced for reliable watermark verification instead conventional correlation-based watermark detection. if authentic, the face pattern can further serve**
***Keywords*— Biometrics, Digital watermarking, Dither.**

I. INTRODUCTION

Fingerprint and face recognition system is the most widely deployed biometric technologies, with a number of distinct dealer offering a wide range of solutions. A number of weaknesses may affect the effectiveness of face and fingerprint recognition in certain cases factors such as finger injuries or manual working can result in certain users being unable to use a fingerprint-based recognition system, either temporarily or permanently. Small-area sensors embedded in portable devices may result in less information available from a fingerprint and/or little overlap between different acquisitions. It is hard to get the fingerprint of one person without direct contact. It is time consuming to search the manual database of fingerprint and face (photo) of a criminal. We cannot use the manual database of face and fingerprint remotely (from branch offices) to get the information needed directly from the location of the manual database; in other word the manual database is not portable.

II. LAPLACIAN EDGE DETECTION

It wishes to build a morphing algorithm which operates on features extracted from target images automatically. It may be a good beginning to find the edges in the target images. Here, we have consummate this by implementing a Laplacian Edge Detector.

Algorithm:

Step 1: Start with an image of a Shark as a sample Fig.1 that is compared with the various types of other Sharks images.

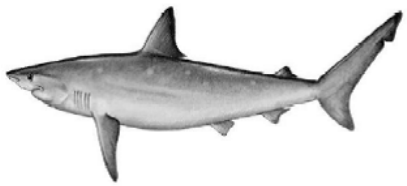


Fig1. Shark image

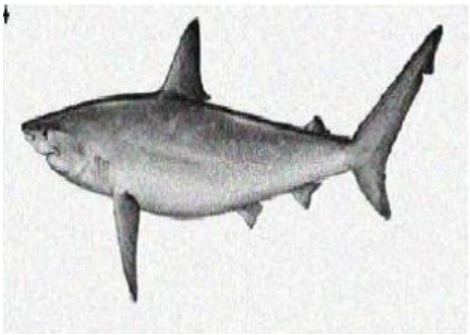


Fig2. Image with noise

©IJRASET 2015: All Rights are Reserved

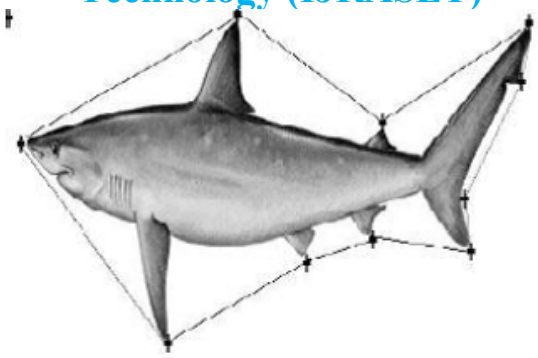


Fig3. Edge detected image

Step 2: Blur the image Fig.2 On identifying the Shark type, the edges are selected for performing a morph, it is not really needed to detect the "every" edge in the image, but only in the main features Fig.3 Thus, the image has been blurred prior to edge detection. This blurring is accomplished by convolving image with a Gaussian.

Step 3: Perform the laplacian on this blurred image. It is necessary to perform the laplacian transformation. For example the laplacian operation is as follows:

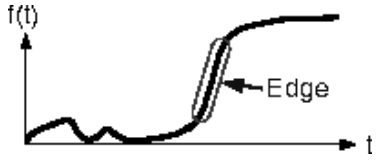
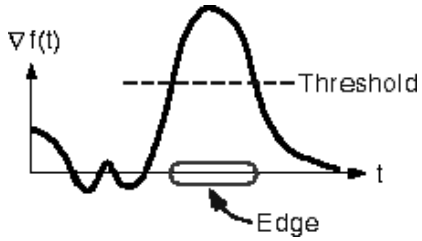


Fig.4First derivative

Fig. 4 shows the gradient of this signal that has been marked which is in one dimension, which is the first derivative with respect to‘t’



.

Fig.5Second derivative

In Fig.5 distinctly it shows the gradient which has a large peak centered on the edge. By comparing the gradient to a threshold, through the edge. Whenever the threshold is exceeded (as shown above). In this case, an edge is found, but the edge has become "concentrated" due to the thresholding. As the edge is occure at the peak, the laplacian operation can be applied in one dimension, it is the second derivative with respect to t and finding the zero crossings

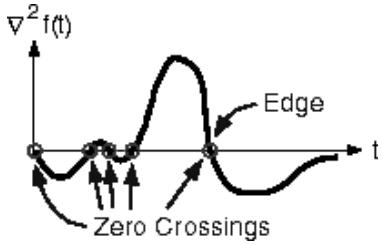


Fig.6 Identification of Zero Crossing

In Fig.6 it depicts the laplacian operation of one dimensional signal. As expected, the edge corresponds to a zero crossing, but other zero crossings are corresponding to small ripples in the original signal which is also marked. In this method the laplacian operation is applied to test the image. In this study, the image of the Shark has been taken for testing the laplacian operations.

©IJRASET 2015: All Rights are Reserved

1) Sobel Operator

The operator consists of a pair of 3×3 convolution kernels as shown in Fig(a)

-1	0	+1
-2	0	+2
-1	0	+1

Gx

+1	+2	+1
0	0	0
-1	-2	-1

Gy

Fig.7

These kernels are designed to respond maximally to edges running vertically and horizontally relative to the pixel grid, one kernel for each of the two perpendicular direction. The gradient magnitude is given by:

$$|G| = \sqrt{Gx^2 + Gy^2}$$

Typically, an approximate magnitude is computed using:
This is much faster to compute.

$$|G| = |Gx| + |Gy|$$

The angle of orientation of the edge (relative to the pixel grid) giving rise to the spatial gradient is given by:

$$\theta = \arctan(Gy/Gx)$$

III. SYSTEM MODEL

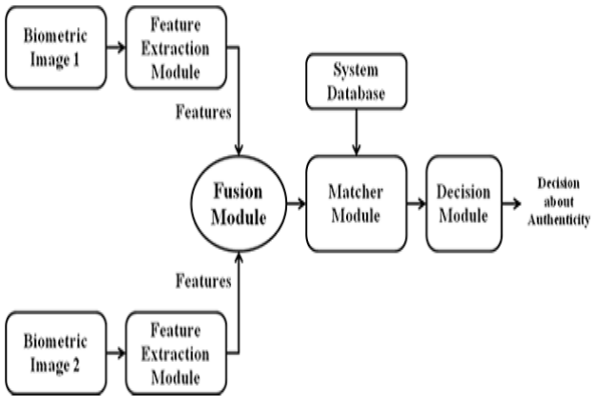


Fig.8 System Architecture

A. Enrollment Process:

The stages of proposed enrollment process for multimodal biometric templates are below:

Step 1 : Read the _ngerprint image and face image as watermark biometric image.
Step 2: Then create measurement Vector of watermark biometric image using its transformation and measurement matrix.
Step 3 : Then plunge this measurement Vector of biometric watermark information into face biometric image of same individual and generate watermarked multimodal biometric image.
Step 4: Cache the watermarked version of multimodal biometric template at system store database.

B. Authentication Process:

©IJRASET 2015: All Rights are Reserved

When any individual try to entering in organization, then _rst step is enrolled individual biometric data and stored at system database. at the Next time when individual biometric queries is coming then takes two biometric templates of individual which predefined according to an algorithm.

Step 1 : Take the Fingerprint and face image of same individual as biometric queries.
Step 2 : Generate watermarked version of face biometric queries using fingerprint as watermark data of same individual using watermark embedding algorithm.
Step 3 : Then compare this watermarked version of face biometric queries of individual with enrolled data of same individual using matching module where face recognition algorithm is used.
Step 4 : If matching score is greater than threshold value of matcher module then extracted measurement vector data of fingerprint biometric watermark from watermarked face biometric image.
Step 5 : Then regenerate fingerprint watermark image using CS theory reconstruction algorithm and compare extracted fingerprint image with enrolled fingerprint biometric data of same individual using fingerprint recognition algorithm.
Step 6 : If matching score is greater than threshold value then individual is allowed to enter the system

IV. DIGITAL WATERMARKING TECHNIQUE

A. What is watermarking?

Digital watermarking is the act of hiding a message related to a digital signal (i.e. an image, song, video) within the signal. It is a concept closely oriented to the technique in which we hide the data behind the image i.e steganography, in that they hide a message inside a digital signal. However, what separates them is their aim. Watermarking tries to shield a message related to the actual content of the digital analog signal, while in steganography the digital analog signal has no relation to the text, and it is merely used encover its existence.
Watermarking has been around for several decades, in the form of watermarks found startingly in plain paper and subsequently in paper chits. However, the area of digital watermarking was only developed during the last 15 years and it is now being used for many different applications.
In the following sections I will present some of the most important applications of digital watermarking, explain some key properties that are adorable in a watermarking process, and give an review of the most common models of watermarking . These basic models will be further illustrated by the use of example watermarking systems that were developed in Matlab. All images used in this essay, excluding those used to present the results of the example watermarking systems are taken from this book .

B. Watermarking applications

The increasing amount of research on watermarking over the past decade has been largely driven by its important applications in digital copyrights management and protection.
One of the first applications for watermarking was broadcast auditing. It is often essentially important that we are able to track when a specific video is being broadcast by a television station. This is most important to announcing agencies that want to ensure that their commercials are getting the air time they compensated for. Watermarking can be used for this goal. Information used to identify individual videos could be embedded in the videos themselves using watermark, making broadcast auditing easier.
Another very important application is owner recognition. Being able to identify the owner of a particular digital process of art, such as a video or image can be slightly difficult. Nevertheless, it is a very important aim, specially in cases related to copyright unfrequent. So, instead of consideration copyright notices with every image or song, we could use watermarking to embed the copyright in the image or the song itself.
Transaction tracking is another interesting application of watermark. In this case the watermark inserted in a digital work can be used to record one or more transactions taking place in the history of a copy of this task. . watermarking could be used to record the recipient of every legal copy of a movie by embedding a different watermark in each replica. If the movie is then reveal to the online network, the movie producers could recognized which recipient of the movie was the source of the leak. Finally, copy control is a very promising application for watermarking. In this application, watermarking can be used to prevent the illegal copying of songs, images of movies, by embedding a watermark in them that would instruct a watermarking-compatible DVD or CD writer to not write the song or movie because it is an illegal copy.

C. Watermarking properties

Every watermarking system has some very important desirable properties. Some of these properties are often conflicting and we are often forced to accept some trade-offs between these properties depending on the application of the watermarking system. The first and perhaps most important property is capable. This is the possibilities that the message in a watermarked image will be correctly detected. We ideally need this probability to be 1. Another important property is the image fidelity. Watermarking is a process that alters an original image to add a text to it, therefore it invariably affects the image's quality. We want to keep this degradation of the image's quality to a minimum, so no obvious difference in the image's fidelity can be noticed. . Every watermarked work is used to receive a message. The size of this message is often important as many systems require a relatively big payload to be embedded in a cover work. There are of course applications that only need a single bit to be embedded. The false positive rate is also very important to watermarking systems. This is the number of digital works that are identified to have a watermark embedded when in fact they have no watermark embedded. This should be kept very low for watermarking systems. Lastly, robustness is crucial for most watermarking systems. There are many cases in which a watermarked work is altered during its lifetime, either by transmission over a lossy channel or several malicious attacks that try to remove the watermark or make it unpredectable.

V. WATERMARKING MODELS

There are several ways in which we can model a watermarking method. These can be broadly categorised in one of two categories. The first category contains models which are based on a communication-based view of watermarking and the second category contains models based on a geometric view of watermarking. In the rest of this essay, I only refer to image watermarking because I only concentrated on images during the development of example watermarking systems.

©IJRASET 2015: All Rights are Reserved

A. Communication-based models

Communication-based models describe watermarking in a way very similar to the traditional models of communication systems. Watermarking is in fact a process of communicating a message from the watermarking embedder to the watermarking receipent. Therefore, it makes ideas to use the models of secure communication to model this process. In a general secure communication model we would have the sender on one side, which would encode a message using some kind of encoding key to prevent eavesdroppers to decode the message if the message was intercepted during transmittal. Then the text would be transmitted on a communications channel, which would add some noise to the noise to the encoded text. The resulting noisy text would be received at the other end of the transmission by the receiver, which would try to decode it using a decoded key, to get the original text back. This technique can be seen in fig.9

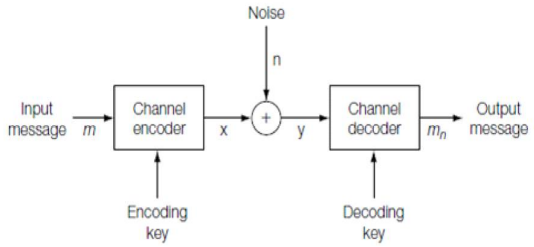


Fig.9 Standard model of a communication channel using decoded key

In general, communication-based watermarking models can be further divided into two sub-division. The first uses side-information to appreciate the process of watermarking and the second does not use side-information at all. The term side-information refers to any auxiliary information except the input message itself, that can be used to better encode or decode it. The best example of this is the figure used to carry the text, which can be used to provide important information to enhance the correct detection of the message at the receiver.

B. Geometric models

It is often useful to think of watermarking in geometric issues. In this type of technique, images watermarked and unwatermarked, can be seened as high-dimensional vectors, in what is called the media area. This is also a high-dimensional area that contains all possible images of all dimensions. For example a 512 X 512 image would be described as a 262144 elements vector in a 262144-dimensional space. Geometric models can be very useful to better visualize the watermarking process using a number of regions based on the desirable properties of watermarking. One of these areas is the embedding region, which is the region that include all the possible images resulting from the embedding of a message inside an unwatermarked image using some watermark embedding technique. Another very crusial region is the detection area, which is the area containing all the possible images from which a watermark can be successfully extracted using a watermark detection algorithm. Lastly, the region of acceptable fidelity contains all the possible images resulting from the embedding of a message into an unwatermarked image, which essentially look identical to the original image. The embedding region for a given watermarking system should ideally lie inside the intersection of the detection region and the region of acceptable integrity, in order to generate successfully detected watermarks that do not alter the image quality very much.

An example of a geometric model can be seen in Figure.10. Here we can seen that if mean square error (MSE) is used as a measure of integrity, the region of acceptable integrity would be an n-dimensional sphere centred on the original unwatermarked image (co), with a radius defined by the largest MSE we are willing to accept for images with acceptable integrity. The detection area for a detection algorithm based on linear correlation would be defined as a half space, based on the threshold used to decide whether an image has a watermark embedded or not. Note that the diagram is merely a projection of an n-dimensional space into a 2d space.

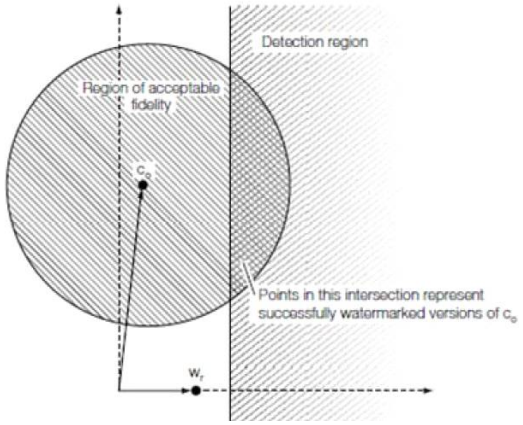


Figure .10 The region of acceptable fidelity (defined by MSE) and the detection region (defined by linear correlation)

When thinking about complex watermarking process, it is sometimes useful to consider a projection of the media space into a possibly lower-dimension marking space in which the watermarking then takes place as usual. This projection can be handled more easily by computers

©IJRASET 2015: All Rights are Reserved

because of the smaller number of vector elements and can be possibly expressed by block-based watermarking algorithms which separate images into blocks instead of operating on a pixel basis.

VI. DIFFERENTIATION OF DIFFERENT EDGE DETECTION ALGORITHMS

Figure.11 Image used for edge detection analysis

Edge detection of all four types was performed on Figure.11 Canny yielded the best consequences. This was expected as Canny edge detection accounts for area in an image. Canny yields thin lines for its edges by using minimal suppression. Canny also use hysteresis with thresholding.

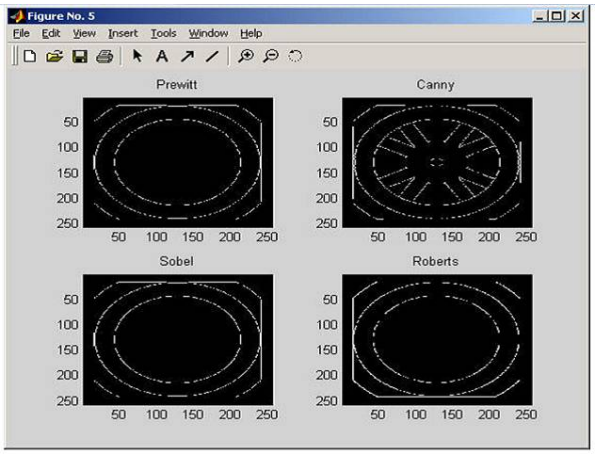


Figure. 12Results of edge detection on Figure 4(a). Canny had the best results

Figure .13 Comparison of Edge Detection Techniques (a)Original Image (b) Sobel (c) Prewitt (d) Robert (e) Laplacian (f)Laplacian of Gaussian.

VII. CONCLUSIONS

In this paper, we have proposed a watermarking based two-stage authentication framework to enhance biometric security and performance. It is theoretically appropriate for any biometric trait(s), and the two-stage strategy could be modified flexibly

©IJRASET 2015: All Rights are Reserved

(either cascaded for filtering out samples with large difference, or parallel: multimodal fusion authentication) according to the application requirements. Moreover, due to the easy acquisition and good integration with future human-machine interaction technologies, the gesture trait might also greatly broaden the application of biometric watermarking.

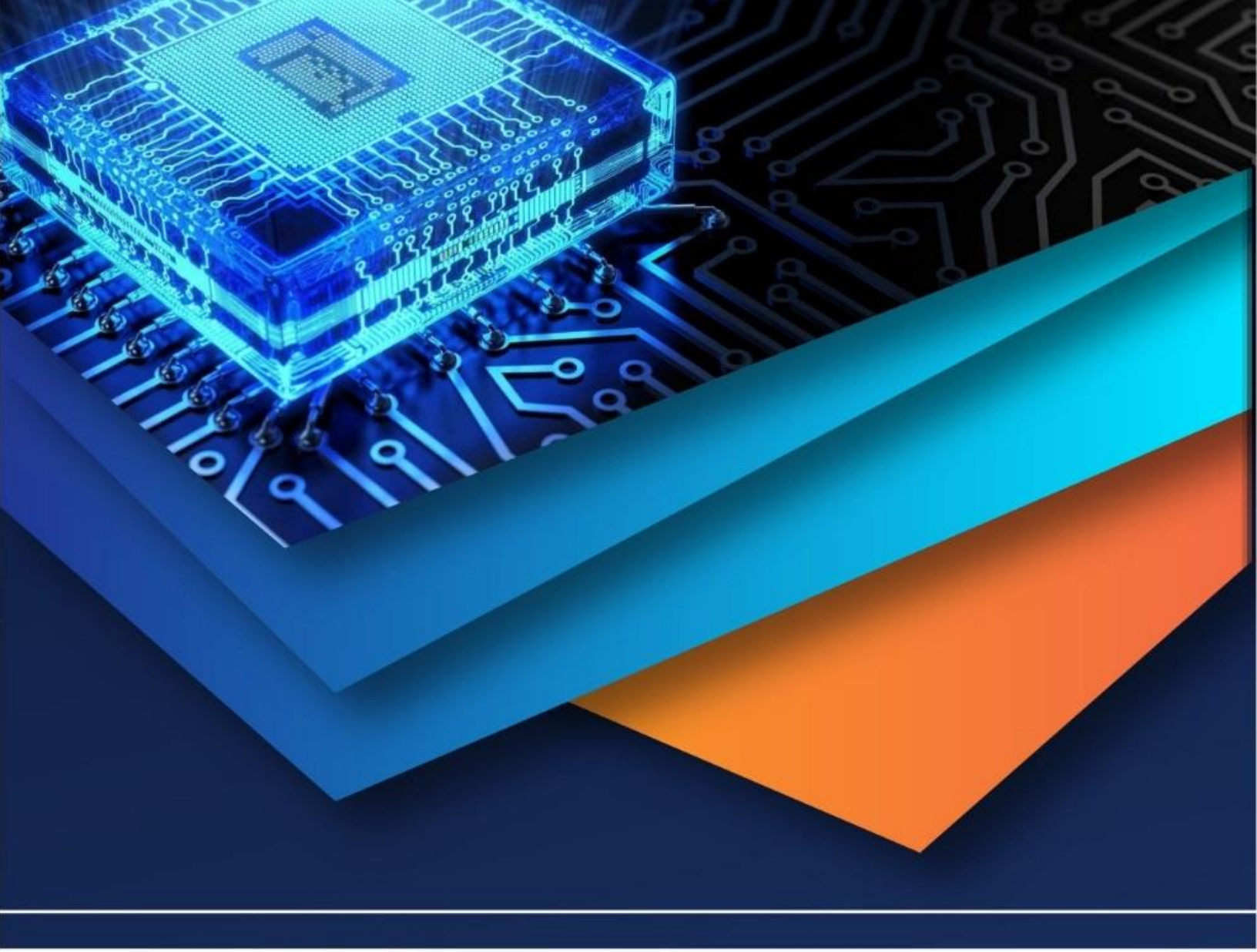
ACKNOWLEDGMENT

We could never have completed our project without the support and assistance of many person. First and foremost, we would like to explicit deepest gratitude to our project guide Prof J. Y. Kapadnis for his excellent guidance, valuable suggestions and kind of encouragement in academics. We are grateful for his help. We are thankful to our HOD Prof. M. T. Jagtap and Principle Prof. Dr. N. S. Walimbe for providing us this infrastructure and labs. Last but not the least we owe a debt to our parents who are the silent guides in our life. We are also thankful to all our friends for their encouragement and support.

REFERENCES

[1] Chen, L., "Laplacian Embedded Regression for Scalable Manifold Regularization",IEEE Transactions, Volume: 23, pp. 902 – 915, June 2012.
[2] Chunxi Ma, et.al.; "An improved Sobel algorithm based on median filter", convention of Electrical and Electronics Engineers, 2nd International IEEE conference, China, Volume: 1, pp. 88-93, Aug 1, 2010.
[3] D. Mintz, "Robust Consensus Based EdgeDetection", CVGIP: Image Understanding, Volume 59, Issue 2, March 1994, pp. 137–153, 26 April 2002.
[4] Nick Kanopoulos, et.al. ; "Design of an Image Edge Detection Filter using the Sobel Operator", Journal of Solid State Circuits, IEEE, vol. 23, Affair: 2, pp. 358-367, April 1988.
[5] Seif, A.,et.al. ;"A hardware architecture of Prewitt edge detection", Sustainable Utilization and Development in Engineering and Technology (STUDENT), 2010 IEEE Conference, Malaysia, pp. 99 – 101, 20-21 Nov. 2010
[6] T.G. Smith Jr., et.al. ; "Edge detection in images using Marr-Hildreth filtering techniques", Journal of Neuroscience Methods, Volume 26, Issue 1, pp. 75–81, November 1988.

©IJRASET 2015: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)