International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-1S, October 2019

Digital Ownership by Biometric Watermarking

P. Valarmathie, A. Manju, R. Mervin

Abstract* — Digital watermarking is a digital data that can be embedded in digital documents, images, audio and video. This watermark technique uses the unique biometric data of individuals. The individuals biometric of eye, vein and fingerprint is embedded in the digital image. These unique data are fused and encrypted. The fusion of three biometric data is output as a digital image. The host image is processed for embedding the fusion image in it. The process of embedding image in another image is watermarking. It is also the domain of image processing. Generally it means hiding an image in the host image. It is a technique to secure the unique data of owner in an image to prove the ownership of the owner. Watermarking the unique features in a digital image establish that the digital image is belongs to the user whose biometric data watermarked. The watermarking process is robust and perceptual transparency. The unique biometric data will logically prove the ownership of digital media.

Keywords*— Watermarking, Digital ownership, Multimodel biometric, Image processing.

I. INTRODUCTION

It is the century where billions of information are created every second with the supremacy of internet and digital data such as images, audio and video files. In this era most of the data are digitalized and stored. There is no proof for the digital information in internet which all circulating all over the world. There will be no decrease in the creation of digital media. Reproduction of these digital data is very easy due to the ownership of the digital document. Digital watermarking is the solution for the problem of losing digital media, which helps to fix the issue of ownership of the digital media. Digital ownership is a technique and a tool used to copyright the digital data. Some of the watermarking method proposed with the biometric of a user. Biometric data is the only data without the same features for two different persons. Even the identical twins don’t have the same biometric feature. It varies to each person; it is the best data uses for the ownership. Multimodel biometric systems are the pattern recognition systems, which identifies an individual physiological or behaviour characteristic like face, vein, iris, voice, palm, retina and fingerprint. In this digital watermarking to recognize discrete individuals, multiple biometrics likes iris, fingerprint and vein are used. This technique provides a recognition rate higher in comparison to biometric systems that relay on a single biometric feature. The major aim of this paper is to study the watermarking technique for digital ownership.

II. RELATED WORK

A pseudorandom number sequence or chaotic sequence is used for generating a watermark. The digital ownership of a watermark is an issue that has not been addressed in the present methods. In case of piracy of the digital media will be difficult to prove ownership of a digital watermark [1]. The dispute of ownership for digital media will define it is not physically owned. Digital ownership is the solution for the copyright protection for digital media. A watermarking will be present permanently in the original data. Even when the data has a circulation and reproduction [2]. The watermark implanted regions are selected in the high-energy regions. It makes the embedded image robust against signal processing attacks. To sustain the processing attacks and to be secure the watermark needs to have the requirements of perceptual transparency and robustness. Perceptual transparency means that the visibility of an image is not changed due to a watermark embedded in the host image [3]. Robustness means the implanted watermark survives even when the image undergoes through signal processing attacks like histogram, filtering etc. Only Authorized persons should be able to detect the watermark image [4]. when two or more images are spliced together to create convincing image forgeries, geometric transformations, such as resizing and rotation, are almost always needed. In recent years, researchers have developed many digital forensic techniques to identify these operations [5]. Previous works in this area focuses on the analysing of images that have undergone single geometric transformations, e.g., resizing or rotation. In several recent works, researchers have addressed yet another practical and realistic situation: successive geometric transformations, e.g., repeated resizing, resizing-rotation [6]. The biometric system can be roughly sketched and consists of a sensor module, a feature extractor module, a matcher, a database, and an application device which is driven by the matcher output. In a feature transformation approach, a function that is dependent on some identification parameters, which can be used as a key an it is applied to the input biometric to generate the protected templates. The employed function can be either invertible, resulting in a salting approach. When a one-way function is applied to the template and it is computationally hard to invert the function even if the transformation parameters are known [7].

Manuscript published on 30 October 2019.
* Correspondence Author (s)

Dr. P. Valarmathie, Professor, Saveetha Engineering College, Chennai, India.
A. Manju, Assistant Professor in Saveetha Engineering College, Chennai, India.
Dr. R. Mervin, Professor in Saveetha Engineering College, Chennai, India.

Retrieval Number: A10331091S19/2019©BEIESP
DOI:10.35940/ijeat.A1033.1091S19
Journal Website: www.ijeat.org

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

III. BIOMETRIC WATERMARKING

In the previous method used the pseudorandom number sequence and watermark the unibiometric of the user. Which is easy to piracy the single biometric, it is not secure enough. Also the system can question the digital ownership of the digital media with this watermark. To increase the security and reduce the issue of the digital media ownership multi-biometric is used. This put forwards an ownership of digital images by implanting unnoticeable digital pattern in the image. The biometric features of more than one subject are used for creating the digital pattern. So, the identification of individual using single biometric is not accepted. This study uses the discrete wavelet transformation for the identification of the region where the image can be embedded in the host image. Also, the encryption of the biometric image uses the arnold cat map, a chaotic encryption. Experimental results indicate the image sustains signal processing attacks and the image does not change the perceptual properties of the image. The extraction of the digital image proves the ownership of the digital image with unique identification. The process involved in digital biometric watermarking is shown by the block diagram below.

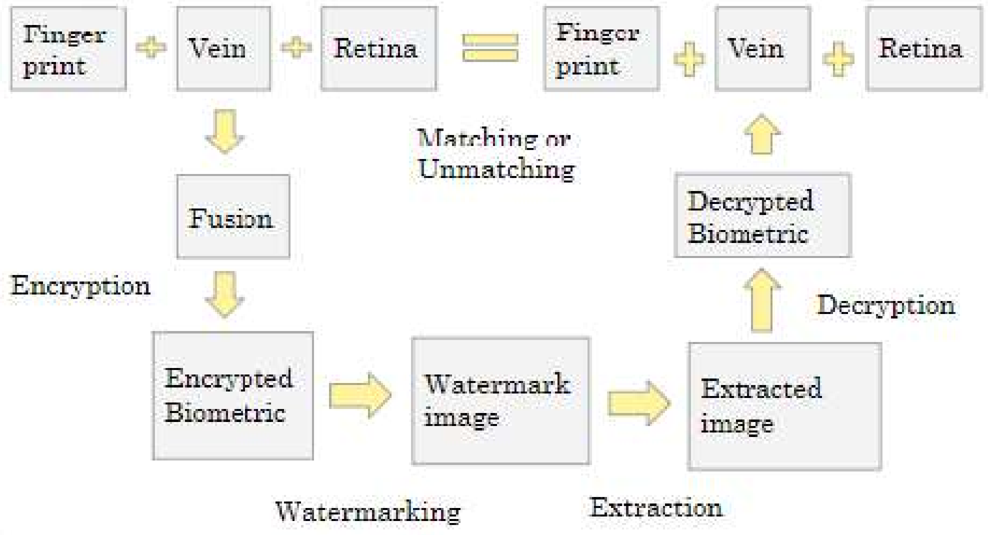


Fig: Digital Biometric Watermarking

A. Multi-Model Biometric Fusion

Using the users biometric like fingerprint, iris and vein, each individual feature get pre-processed. These processed images of biometric segmented for the fusion. It makes the three individual segmented images into single fusion image, which overlap on each other, display as single segmented image. The segmented output of vein and retina get multiplied into single segmented image. It is then multiplied with another segmented output of fingerprint. This process of multiplying the segmented images will results in the segmented output as a single image which is the fusion of three biometric segmented images. The segmentation of the image is measured with region based, edge based, threshold, feature based clustering, model based. Fingerprint image is segmented using the edge based segmentation. Using the canny edge detection and ridge identification procedure the segmentation of finger print developed. Iris photography and feature extraction is a long process and it demands light controlled ambience which may be a hefty process. Then compare imaging of fingerprint is easy and cheap. Same as the finger and iris segmentation vein also have the segmentation part before the fusion of images.

B. Chaotic Encryption.

To ensure the security of the multi-biometric image encryption process is done. Encrypting the image will protect the image safe. Arnold cat map technique is used for the encryption process. It employs the shearing and wrapping operation to completely scramble a matrix after several iterations. It is a one to one mapping technology. The mathematical representation of Arnold cat map for a matrix of size N × N is

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = A \begin{bmatrix} x_n \\ y_n \end{bmatrix} \pmod{N},$$

Where A = $\begin{bmatrix} 1 & b \\ a & 1+ab \end{bmatrix}$ is transformation matrix.

The determinant of transformation matrix [A] = 1, a and b are positive integers and a, b <= N and N>1. Where N is the modulo of the map (1). The general cat map at a=b is described according to the following formula:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = A \begin{bmatrix} x_n \\ y_n \end{bmatrix} \pmod{N},$$

Where A = $\begin{bmatrix} 1 & b \\ a & 1+ab^2 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & a \end{bmatrix}^2$,

And $x_{a,}$ y_a €{0,1,2,3…….N-1}. Arnold cat map has been used to iterate a fusion image for encryption which is used as a watermark. This encryption process for the image, it will increase the security. The encrypted image will be safe and secure for piracy of that embedded watermark image. The stealing of the ownership will be prohibited using this process.

Retrieval Number: A10331091S19/2019©BEIESP
DOI:10.35940/ijeat.A1033.1091S19
Journal Website: www.ijeat.org

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

C. Watermarking

In the watermarking an image in a host image, a specific region should be identified, where the embedding image should be watermarked. To identify the embedding region in host image, discrete wavelet transformation is used. This transformation allows good localization both in time and frequency domain and provides frequency information in a stable form.

DWT is one of the domains that analyze signal at multiple levels. There are other than DWT such as DCT, SVD and so on.

A two dimensional image is converted into single DWT, image is divided into four sections, one section is a low frequency of original image, the bottom left section is the vertical details of the original image, the top right contains horizontal detail of the image, the bottom right block contains high frequency of original image, again compare the second level of the DWT of the image.

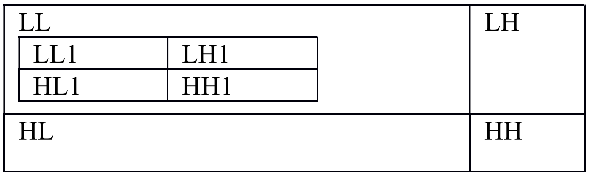


Fig: DWT Decomposition

The low frequency coefficient contains major information of the host image. The embedded image should be watermarked in the low-low level for the image robustness. It is more robust to implant watermark in that level. The watermark to be robust against the compression it is necessary to choose the specific position to watermark. So, it is necessary to choose the low frequency of DWT to watermark. This image is sectioned into blocks of size 8x8.

D. Feature Extraction

Feature extraction is done after the preprocessing image. The process of extraction is divided into two general stages, namely, feature selection and classification. This method will increase the image stable. Haar wavelet technique is used to extract features from the iris image. The minutiae feature in fingerprint such as ridge ending and ridge bifurcation. This method improves both the usability and reliability. The pre-processing and the level of segmentation has been achieved, some feature extraction is followed. It focusses on the extraction to observe the impact on the efficiency of the recognition system. The extraction of feature points of each image is required for the further process. This helps for matching the biometric feature points. Which points and values are the final check of the matching to ensure the ownership of the watermark embedded image.

E. Feature Matching

After feature extraction process then matching with the users unique biometric is done. It is accessed only by the matched biometric owner. It is unique and the matched biometric user is the owner of the digital image and proves the digital ownership. Feature matching is calculated using the Euclidean distance with the fused output and haar transformation. The distance between two pixels at coordinates (x_1,y_1) and (x_2,y_2). The Euclidean distance is given by

$$\sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}$$

The distance acquired between the coordinates identifies the matching. The coordinates gives the long distance match then it is unmatched. If the distance is close with the coordinates then it is matched. Then the available values of input and output features should match each other.

In this feature matching the decrypted image is matched with the original biometric images of the owner to verify the copyright of ownership using PSNR with the decrypt image. This is process to verify the ownership of an image. If the distance value is nearly equal indicates the matched output and if it is opposite then it is unmatched output.

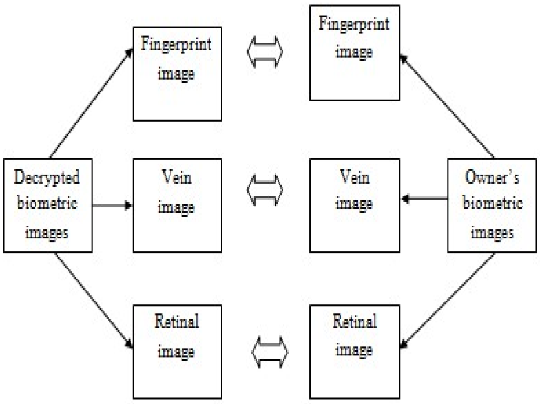


Fig: Feature matching process

IV. RESULT AND DISCUSSION

This paper suggest a secure watermarking by using encrypted vein, iris and fingerprint fusion image. Such digital watermarking technique helps in the digital ownership of the digital media. The digital watermark ensures the ownership of the watermark and the encryption ensures that the biometric data is not exposed to any threat or third party vulnerability. The validation of such encrypted biometric watermark has been recovered using discrete wavelet transformation based watermarking method. It is robust and safe from the signal processing attacks. The feature points extracted from the recovered watermark has been uniquely identified and also mapped for identification. This is clearly indicates a significant development in identification and proof of ownership of digital media. According to the previous results analysis, we analyzed specific periodic traces hidden in digital images that have undergone successive geometric transformations, e.g., repeated resizing, repeated rotation, or rotation-resizing. Specifically, we presented an in depth analysis in the frequency domain of the second-order statistics of the geometrically transformed images. The main contribution of the paper is an exact formulation of how parameters of successive geometric transformations influence the appearance of periodic artifacts and the derived expected positions of characteristic re-sampling peaks. This paper will do the authenticate the ownership of the digital media. The final output of the modules is showed with the snapshots.

The finger image is preprocessed and segmented for the visible of vein.

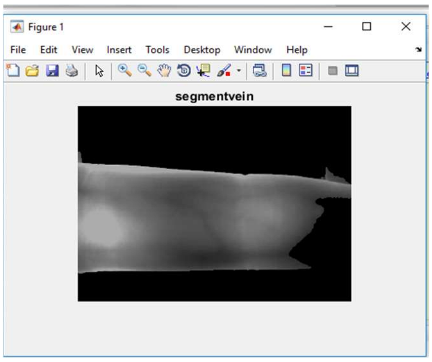


Fig: Segment Vein

Retina is grey channeled and segmented to visible the blood vessels.

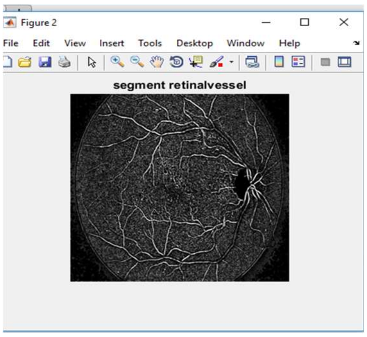


Fig: Segment Retina

The fingerprint is preprocessed and segmented for the feature points.

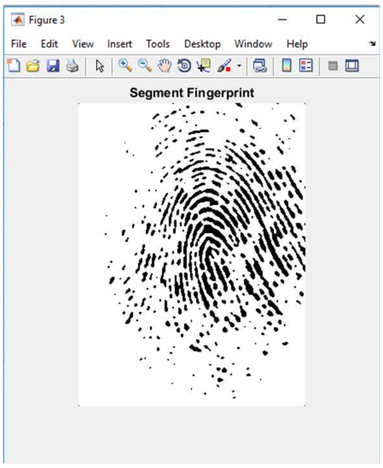


Fig: Segment Fingerprint

Each segmented biometric output is fused to form a single image.

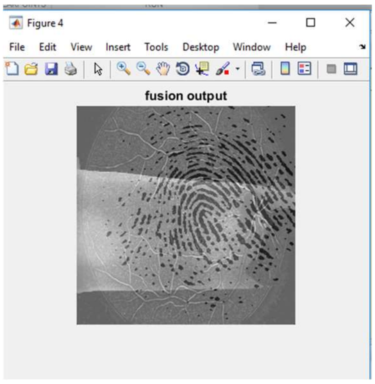


Fig: Fusion Output

The encryption takes the several iterations when it is completed the output of the encrypted image is below.

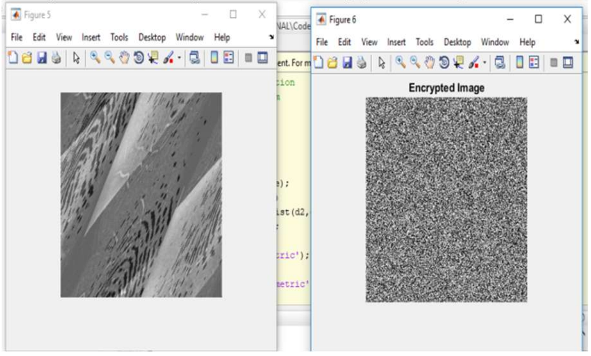


Figure 5
File Edit View Insert Tools Desktop Window Help
Figure 6
File Edit View Insert Tools Desktop Window Help
Encrypted Image

Fig: Encrypted Image

The encrypted output gets watermark in an image, the screen shot is below.

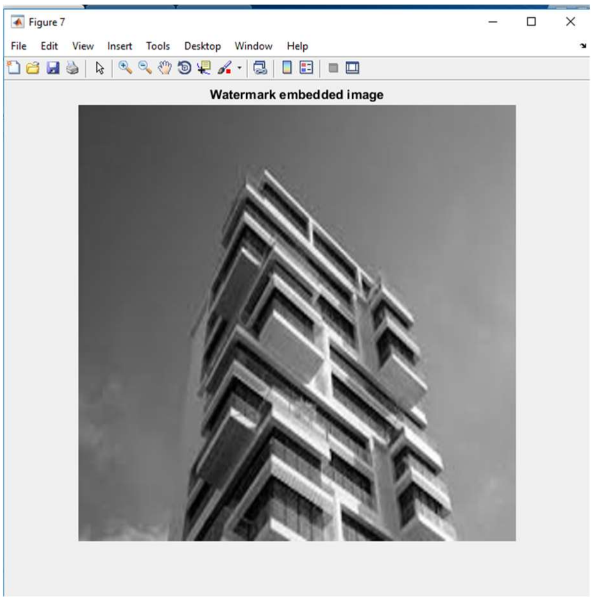


Fig: Watermarked Image

The extracted image is with a little noise and unstable due to the signal attack.

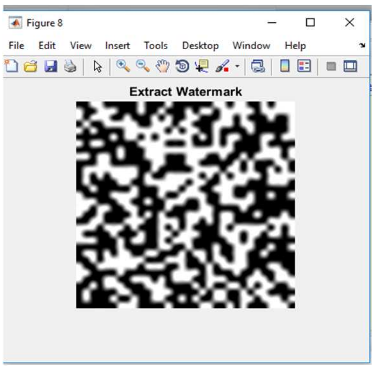


Fig: Extracted Watermark

The decryption is the reverse process of encryption, after several iterations the decrypted output image is showed below.

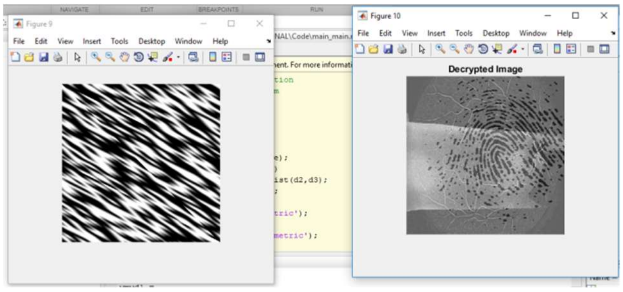
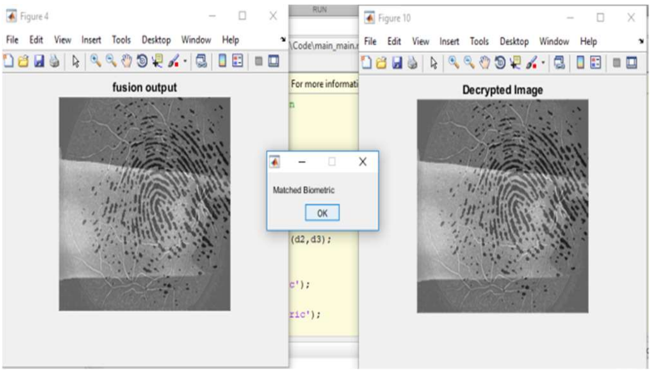


Fig: Decrypted Image

The decrypted is compared for the ownership, the matched output is below.

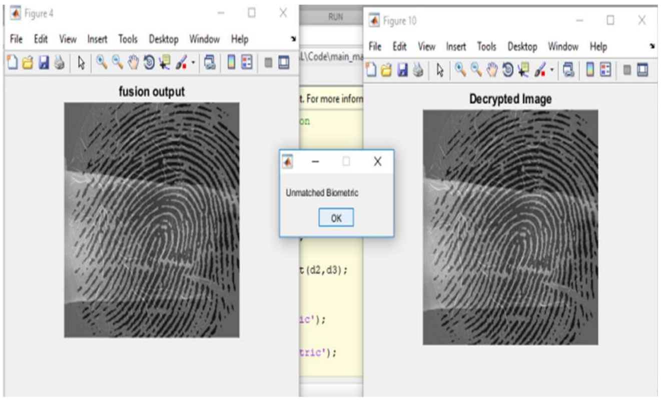


Matched Biometric

OK

Fig: Matched Biometric Output

When the decrypted and owner fused biometric doesn't match then it is unmatched biometric showed below.



Unmatched Biometric

OK

Fig: Unmatched Biometric output

V. CONCLUSION

This watermarking will be the authentication of the watermarked image to the respective owner of that digital media. The digital watermark ensures the ownership of the watermark and the encryption ensures that the biometric data is not exposed to any threat or third party vulnerability. Such digital watermarking technique helps in the digital ownership of the digital media. This is clearly indicates a significant development in identification and proof of ownership of digital media. Future scope may deal to find other efficient ways of encryption and other biometric traits may be explored for generating digital watermark. It is applied to different digital media such as audio, video and documents.

REFERENCES

1. Agbaje MO, Awodele O, Ogbonna AC (2015) "Applications of digital watermarking to cyber security (Cyber Watermarking)", Proceedings of Informing Science & IT Education Conference (InSITE), pp 1–11
2. Chenglong Chen, Jiangqun Ni, Zhaoyi Shen, and Yun Qing Shi (2017) "Blind Forensics of Successive Geometric Transformations in Digital Images", IEEE Transactions on Image Processing, Vol.26, pp.2811 – 2824
3. Emanuele Maiorana, Patrizio Campisi, Julian Fierrez, Javier Ortega-Garcia, and Alessandro Neri (2010) "Templates for Sequence-Based Biometrics with Application to On-line Signature Recognition", IEEE, Vol.40, pp.525 - 538
4. Georgios Goudelis, Georgios Tsatiris, Kostas Karpouzis, Stefanos Kollias (2017) "Transform based feature extraction for effective human action", Computational Intelligence and Games (CIG)
5. K. Nandakumar, A. K. Jain and S. Pankanti (2007) "Fingerprint-based Fuzzy Vault: Implementation and Performance", IEEE Transactions on Information Forensics and Security, vol. 2, no. 4, pp. 744–757
6. Lai C-C, Tsai C-C (2010) Digital image watermarking using discrete wavelet transform and singular value decomposition. IEEE Trans Instrum Meas 59(11):3060–3063
7. Meta Malonia, Surendra Kumar Agarwal (2016) "Digital Image Watermarking using Discrete Wavelet Transform and Arithmetic Progression Technique", IEEE
8. Malay Kishore Dutta, Phalguni Gupta and Vinay K.Pathak (2010) "Blind Watermarking in Audio Signals using Biometric Features in Wavelet Domain", IEEE Region 10 Conference
9. P.Vignitha, Ch. Sai Theja Swaroopa, TVL. Kalyani (2013) "Digital Watermarking using Biometric Feature", Contemporary Computing (IC3), Sixth International Conference
10. SaeidFazli, MasoumehMoeini (2016) "A robust image watermarking method based on DWT, DCT, and SVD using a new technique for correction of main geometric attacks", Vol.127, pp.964-97
11. V. Evelyn Brindha (2011) "Biometric Template Security using Fuzzy Valut", Consumer Electronics (ISCE), IEEE 15th International Symposium.

AUTHOR PROFILE

Dr. P. Valarmathie received Doctor of Philosophy in Data Mining from Anna University in the year 2013. She is currently working as Professor in Saveetha Engineering College, Chennai, India. Her main research area includes Data Mining, Big Data Analytics, Cloud Computing, Semantic Web Services and Network Security. She has 18 years of teaching experience including 6 years of research. She has coordinated in NPTEL Certification programs and DSIR Research Recognition. She has certified EMC Academic Associate in Data Science & Bigdata Analytics and also certified Programming for Everybody (Python), Python Data Structures from Coursera.

A. Manju received Master degree from Anna University in 2008. She is currently working towards Ph. D degree at Saveetha University. She is currently working as Assistant Professor in Saveetha Engineering College, Chennai, India. She has 11 years of teaching experience with good programming skills. She has certified EMC Academic Associate in Data Science & Bigdata Analytics and also certified Programming for Everybody (Python), Python Data Structures, Using Python to Access Web Data and R Programming from Coursera. She completed the online training course Big Data Fundamentals from Big Data University.

Dr. R. Mervin received Doctor of Philosophy in Computer Science and Engineering from B.S. Abdur Rahman Crescent Institute of Science and Technology in the year 2019. She is currently working as Professor in Saveetha Engineering College, Chennai, India. Her main research area includes Data Mining, Big Data Analytics, Cloud Computing, Semantic Web Services and Network Security. She has 16 years of teaching experience. She has certified EMC Academic Associate in Data Science & Bigdata Analytics and also certified Programming for Everybody (Python), Python Data Structures from Coursera.