Steganography for retinal biometrics

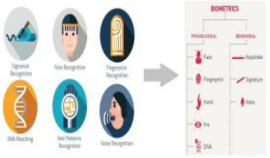
Krishnaraj Chadaga, Srikanth Prabhu , Musica Supriya

Abstract: The retinal pattern biometrics varies to every individual and it is one of the most efficient form of identification. Retinal scanners use infrared rays along with non-invasive color retinal cameras and are very effective in getting a retinal image. We differentiate retinas using segmentation of retinal vascular branch.Further Bifurcation and cross over points are used Steganography is the art of hiding information within another file which can be image, video, audio, text etc. After getting the retinal details, steganographic methods are used to transfer this file securely over the internet. Once received at the receiver, it can be used for verification of user authenticity

Keywords : Biometrics, non-invasive, vascular branch, bifurcation, cross over points, geometric hashing, steganography

I. INTRODUCTION

Identifying a person through his different biological features (fig 1) is the current trend in authentication. Knowledge based methods like user id, password, object-based methods like tokens are not efficient against attackers. Biometric data can't be changed easily as it is different to every individual. Many industries, colleges, hospitals, military and other government agencies are implementing biometrics. Many mobiles are already using finger print authentication. This data should always remain confidential as it is required for further communication. We also have to remember those tedious passwords. There are various biometric data like DNA, earlobes, iris, retina, hand geometry, odour, signature recognition, typing style, vein structure, voice recognition [1,2,3,4]. A survey is found from [5,6,7,8,9].



Different types of biometrics

DNA: DNA is mostly encountered in health care institutions. It is based on genetic characteristics like chromosomes

Ear: Depends on the shape of the ear. Pattern recognition and image processing are used in this process

Eyes-iris recognition: Iris determines the color of the eye. The different nerve patterns can be converted into code for authentication Face recognition: Facial features are used for recognition. Eigen face principles can be used

Eyes-retinal recognition: Retinal blood vessels are observed which have different patterns

Gait: Walking styles and other behaviour aspects are observed

Finger-prints: Unique ridges and valleys on the surface of the fingers are used for authentication

Odour: authentication is done based on a person's smell

Signature recognition: Analysis of signatures

Voice recognition: voice is used to identify the user

Non-inverse color retinal cameras do not use the principal of pupil dilation and it can be integrated well with biometrics [10]. Non-mydriatic camera is used to get the vascular structure of retinal images [11]. Many retinal biometrics are available but retinal muscular pattern holds a firm grip over the others. The light enters into the eye and the reflection is obtained which is then converted as an image to be sent. Most algorithms are based on image detection as opposed to feature points such as branch, bifurcation and cross over points. Geometric hashing is also used to identify these feature points in blurred images. Information hiding techniques like water marking and steganography are a added bonus along with standard encryption. Cryptography makes data look confusing but will still invite attackers. Cryptography makes the information undesirable but steganography hides the information itself. In water marking when data is changed, a change in water marking will be observed. Steganography is hiding one data in another data. The data to be safe guarded will be present in another data called the carrier data. The data can be text, image, audio, video etc. Usually the carrier file should be large enough to hold the data without disorienting its actual appearance. Figure 2 portraits different type of steganography.[26] Text steganography: Hiding the information as a text message. They are two methods. Linguistic steganography which contains semantic and syntactic methods. It also contains format based which involves line shift coding and word ship coding.

Image steganography: Images are the most popular carrier objects used. There are many algorithms where we hide the information as a specific type of image.

Audio steganography: Audio steganography is used to transfer data by modifying or changing an audio signal. We hide secret text on audio contents

Video steganography: Video is used as a carrier file as they are big in size and data can be transferred very easily

Network steganography: The data will be hidden in the TCP headers and they will be transferred when the tcp packets are being sent in the network layer

Revised Manuscript Received on December 30, 2019.
***** Correspondence Author

Mr.Krishnaraj Chadaga*, Department of Computer Science and Engineering, Manipal Institute of Technology, Manipal.

Ms. Musica Supriya, Assistant Professor, Department of Computer Science & Engineering Manipal. Institute of Technology, Manipal - Karnataka.

Dr. Srikanth Prabhu, Member IEEE, Member ACM, completed schooling from Delhi Public School , Bhilai,

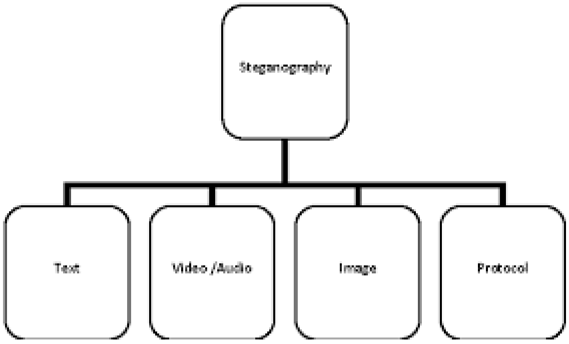


Fig 2. Different types of steganography

II. LITERATURE REVIEW

There are different authentication schemes described in [8,12,14,15,16,17]. These authentication schemes are very different to each other. Some involve marking techniques and the others use a different approach. Eyedentify [13] is available in the market. It maps the vascular pattern using a camera and records up to 192 points. These systems are used in different medical and other government institutions which require high security. In [18] they have a technique called vascular graph. Filters are used in this method. The vascular graph is constructed using different approaches which helps to authenticate. In [14] a method has been used based on fourier transforms to evaluate retinal biometrics. The cosine values are taken into consideration. Template based matching of retinal images was proposed in [15]. Here first a template is constructed and then stored in a data base which can then be compared with a person biometric during the authentication phase In [16] a new technique which involves registration of biometrics using retinal vessel tree. The tree is constructed iteratively and then after the complete construction of the tree, the features are analysed and come to a conclusion. Reference points are taken to get the accuracy. Retinal vascular bifurcation and cross over points were proposed in [15]. Fig 3 shows the bifurcation and cross over points. Deep learning was used in this method. In [20] a network security mechanism was initiated using retinal biometrics. Vessel networks were implemented. Morphological thinning was used in [21], a cryptography key is generated to ensure network security. In [22] they had developed a mathematical method using gaussian derivative for retinal blood vessels. Bifurcation and cross over points are identified as square images. Biometric security framework was developed by [23]. In [24] phase congruency biometrics was used and in [25] retinal vessels were matched using fundus images.

Hisham al Assan in [26] used biometric cryptosystem with steganography using a key exchange algorithm. However very primitive technique has been used. In Biometric key generation technique used in [27]. Hybrid techniques are used to great effect. In [28] face biometrics have been involved with steganography. In [29] a new technique called the discrete wavelet transform has been applied to the retina. This improves the accuracy during steganographic authentication.

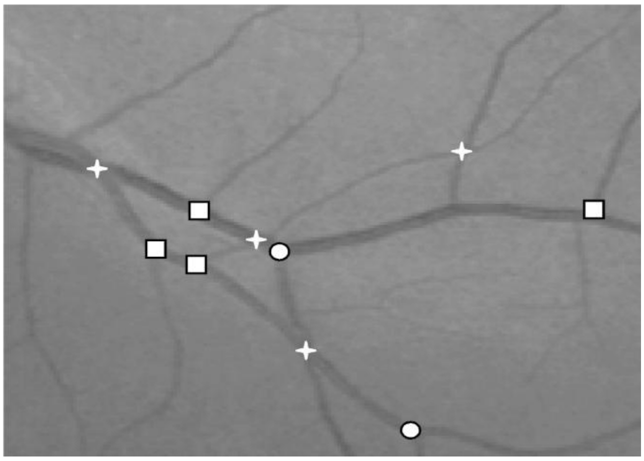


Fig 3. Vascular branch(square), bifurcation(circles), crossover(star) points

III. METHODOLOGY

The retinal scanner will be used to get the raw but accurate images of the retina. The infrared rays will be used for this sole purpose. The retinal images are then converted to YUV images using multiline method[29]. Then we get the image of the optimized retinal data. Image steganography is then applied. The optimized image is embeddded in the cover image and this cover image is sent through the network completely undetected. At the receiver we separate the cover image as well as the optimized image an then this image can be used for further authentication

YUV images: YUV uses the pipeline of color images using a variety of encoding mechanism. Color images are encoded with a person being considered, which allows less bandwidth when it comes to components regarding to chrominance. Transmission errors are reduced compared to RGB mode because of the artifacts related to compression. Interfacing using equipment's related to photographic illusion . Y stands for luminance and the UV for chrominance

The next step is determining the bifurcation points and cross over points from the obtained segmented images. Care must be taken to remove the noise and get the optimized images accurately

Determine crossover points: The number of vessel segment and their angle is calculated. The cross over point each as vertex of the angle and computation of coordinates. We use the formula ($\theta = \operatorname{atan}(dy/dx)$) where dy and dx are differences in the respective axis. Four is the ideal number of segmented vessels and the angle between the retinal vessel structure should be 180∘.Then the values are chosen as follows.[30]

Determine Bifurcation points: From segmented and branch vertices, the bifurcation points are detected based on the children blood vessels as they are easier to detect. The width is expected to be equal so that it is benific and angle less than 90 degree is preferred.

So to identify birfucation points , vessel segment breath should be known.. x is the x coordinate and y is the y coordinate then

$$nx = cx + \sin\theta$$
$$ny = cy - \cos\theta$$

Based on the formulas corresponding bifurcation and cross over points are detected[30]. Figure 5b illustrates this precisely[30]

Steganography: A 2-3-3 LSB technique is used to successfully hide the secret pictures.The cover image should not change when the size of secret image increases.. We embed color retinal secret image into a colored cover image. Using cryptography along with steganography enhances the security. Color space plays an important role in increasing network efficiency and minimizing memory consumption. YUV color space provides reduced bandwidth for chrominance components

Least significant bit: LSB insertion is a easy and practical approach to hide information in a cover image. The LSB(the 8th bit) bit which is changed and we can replace it with a bit from the secret image We can use a16,24,32 bit image , a bit each of green, blue is utilized and represented as a byte. We can store 3 bits in each pixel. Figure 6 shows LSB steganography

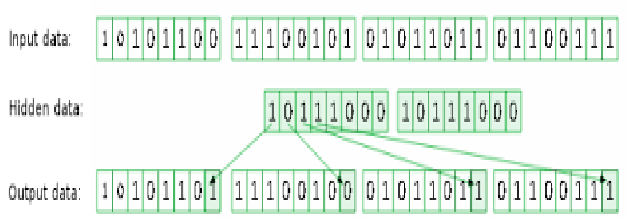


Figure 6 LSB steganography

For a 24 bit image of 3 pixels

(00101101 00011100 11011100)

(10100110 11000100 00001100)

(11010010 10101101 01100011)

We choose a number 200, The binary representation of this number is 11001000 is embedded in the last bit. There will be a new grid given by:

(0010110**1** 0001110**1** 1101110**0**)

(1010011**0** 1100010**1** 0000110**0**)

(1101001**0** 1010110**0** 01100011)

The number is added to the primary 8 bytes of the grid. We should be able to change the 3 bytes itself. In the worst case, to hide a secret image, we only need half the bits if the cover image is big enough. There are 256 ways of selecting different colors. There will be no differences or minute differences if we change the LSB bit. These changes are unrecognizable for human beings. Therefore, the messages can be easily hidden. If the cover image is very large we can use the last bit as well as the bit before that and differentiation is not possible

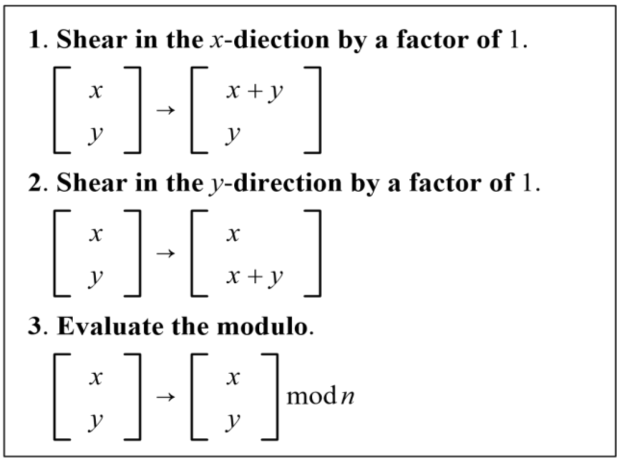
In the example given above, the continuous stream of bytes of the image from the byte in the beginning to the end of the content can be used for information hiding. However, this approach can be easy to detect. The security can be improved in a way by introducing a secret key which deals with the minimum no of pixels to be changed. Even if he comes to know that LSB steganography is used there is no way he can access the image because of the presence of the available secret key

- **LSB and Palette Based Images**

GIF and PNG are available in pallet over the network. Message can be in the palette or into the data of the image. Both the methods have its own advantages and disadvantages. The first method can be used to make the algorithm more secure. If the pallet size is large enough it is an excellent method but on the other hand if the pallet size is small it can affect its efficiency and through put. The second method has more storage space but good security scheme can be a problem. The noise model also has to be considered by using the sensitivity of the color. It is therefore difficult to encode and synchronize.

Encryption

Arnolds catmap technique is used for encryption which strengthens steganography. The knowledge of caos must be known to us. It means disorder, random orientation, disorganization , entropy etc consider an image with x rows and y columns. Using this technique it randomizes the original organization of the pixels. After iterating n times the original image reappears



1. **Shear in the x-direction by a factor of 1.**

$$\begin{bmatrix} x \\ y \end{bmatrix} \to \begin{bmatrix} x+y \\ y \end{bmatrix}$$

2. **Shear in the y-direction by a factor of 1.**

$$\begin{bmatrix} x \\ y \end{bmatrix} \to \begin{bmatrix} x \\ x+y \end{bmatrix}$$

3. **Evaluate the modulo.**

$$\begin{bmatrix} x \\ y \end{bmatrix} \to \begin{bmatrix} x \\ y \end{bmatrix} \bmod n$$

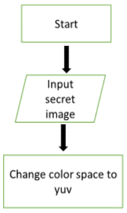


Figure 7 Taking secret image as input

In the beginning we take the secret image which is the segmented retinal image and then we choose a cover image which is three times larger than the secret image. Then embedding of the secret image is done using the 2-3-3 LSB technique. Then the stego image is displayed. The image then travels over the channel through the internet and we receive the secured retinal image at the receivers side. The entire steganographic process is shown in figure 8

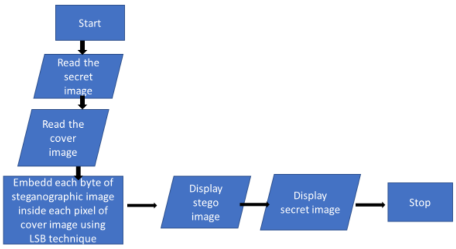

Start
Read the secret image
Read the cover image
Embedd each byte of steganographic image inside each pixel of cover image using LSB technique
Display stego image
Display secret image
Stop

Figure 8 2-3-3 Image steganography

Embedding algorithm

Step1: Read the Secret retinal image.

Step 2: Change shade space of secret image from RGB to YUV.

Step 3: Read cover image.

Step 4 : Embedd each byte of secret image inside 3 pixels of cover image using 2-3-3 LSB technique.

Step 5: Output the stego image.

Extraction algorithm

Step 1: Retrieve secret image from stego image using 2-3-3 LSB technique.

Step 2: Change the secret image from YUV to original color space RGB.

IV. RESULTS AND DISCUSSION

. The snapshots of the system while execution is presented using screenshots. The analysis is done on an image and results are shown using different snapshots and tables

Main Graphical User Interface:

Figure 9 shows the GUI which is displayed when the initial program is executed. It has three buttons. The first button is to select a secret retinal image and change it to YUV color space. The second button is to select the cover image under which retinal image can be hidden. The third button is to create a stego image which is a combination of both

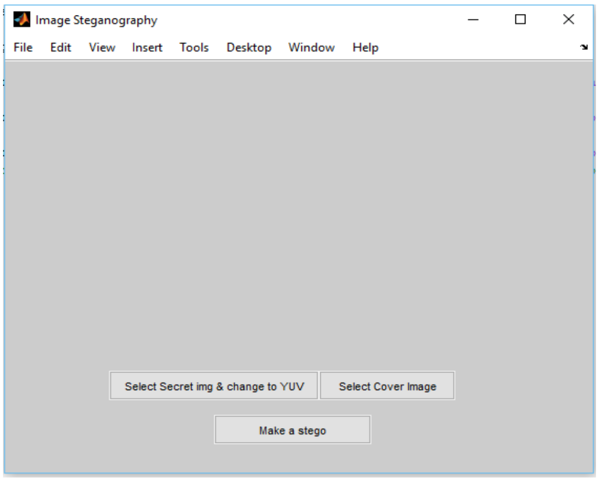


Image Steganography
File Edit View Insert Tools Desktop Window Help
Select Secret img & change to YUV
Select Cover Image
Make a stego

Figure 9 Initial GUI containing 3 buttons

Then we select secret image and change to YUV' button is pressed a folder opens from which we select a secret image and it is then converted to YUV color space. GUI displaying the selected plain secret image and YUV based image is shown.

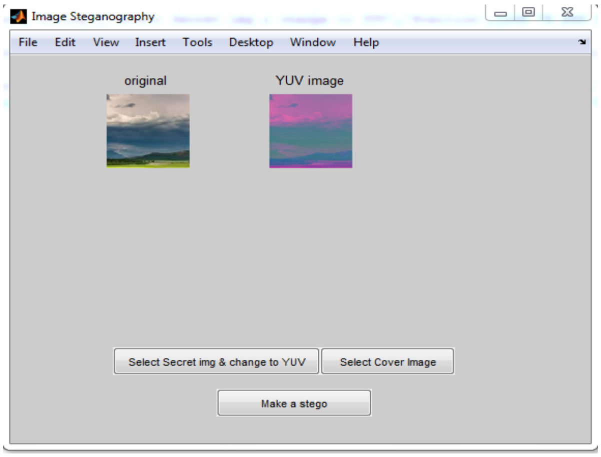


Image Steganography
File Edit View Insert Tools Desktop Window Help
original
YUV image
Select Secret img & change to YUV
Select Cover Image
Make a stego

Fig 10 YUV conversion

Figure 10 shows the window which contains the results. The YUV converted image is placed inside the cover image to make a stego image. From the stego image the hidden image i.e., the secret image is retrieved a to get the converted back original image. There is a button 'Back to Main Screen' which goes back to the initial GUI window

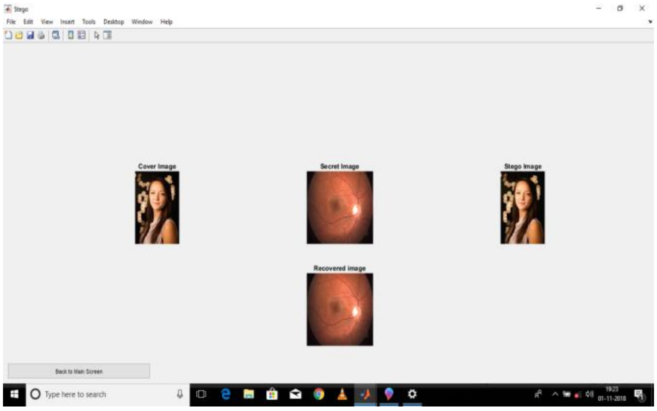


Figure 11 Results

s Normalized absolute error (NAE) computed by a formula and it is a measure of how far the stego image is from the original cover image with the value of zero being the perfect fit.[32] Big value of NAE indicates a dull quality of the resulting image after embedding. The value of NAE is calculated using the Equation.

$$NAE = \sum_{i=1}^{H} \sum_{j=1}^{W} | P(i,j) - S(i,j) | \,/\, \sum_{i=1}^{H} \sum_{j=1}^{W} | S(i,j) |$$

Where H and W are height and width, P(i, j) represents the original image and S(i, j) represents corresponding stego image**.**

Table1: NAE for different secret images

Cover Image	Secret Image	NAE
Image.jpg	Normal.jpg	0.047
Image.jpg	Normal1.jpg	0.045
Image.jpg	Normal2.jpg	0.053
Image.jpg	Normal3.jpg	0.061
Image.jpg	Normal4.jpg	0.034
Image.jpg	Normal5.jpg	0.031
Image.jpg	Normal6.jpg	0.045

V. CONCLUSION

Retina scan has its own advantages. We can get false positive outputs very easily, and it remains throughout a person's life. It cannot be altered very easily because it lies deeply within one's eye. In addition, retinal scan error is very rare ie 1 out of 10000 where as finger print has 2 in 1000. There are some disadvantages too, it is some what uncomfortable to people. Some diseases like glaucoma, diabetes can harm the retinal structure [34] in older population. Retinal scanners are extremely costly compared to other biometric scanners. We also need a lot of training to identify retinal reliability. For the time being it is only used in the defense, FBI etc.

There is more need for security because most of the important transactions are happening over the internet. NAE values in2-3-3 is better than the previous version of 3-2-2. There is a drastic improvement in NAE values. Combining cryptography with steganography provides a better and higher security. YUV color space adds more value to the secret image as the combination of both of them make the image undetectable and even if the image is found then it is very difficult to decrypt the information because of its benific presence

Combining retinal biometrics is an excellent aspect as this extremely confidential retinal configuration of a person can be transferred undetected through the internet

REFERENCES

1. GJain, A.K., Ross, A., Prabhakar, S.: 'An introduction to biometric recognition', IEEE Trans. Circuits Syst. Video Technol., 2004, 14, (1), pp. 4–20
2. de Luis-Garcia, R., Alberola-Lopez, C., Aghzout, O., et al.: 'Biometric identification systems', Signal Process., 2003, 83, pp. 2539–2557
3. Prabhakar, S., Pankanti, S., Jain, A.K.: 'Biometric recognition: security and privacy concerns', IEEE Secur. Priv. Mag., 2003, 1, (2), pp. 33–42
4. Islam, S.M.S., Davies, R., Bennamoun, M., et al.: 'Multibiometric human
5. recognition using 3d ear and face features', Pattern Recogn., 2013, 46, pp. 613–627
6. Bhattacharyya, D., Ranjan, R., Alisherov, F., et al.: 'Biometric authentication: a review', Int. J. u- and e- Serv. Sci. Technol., 2009, 2, (3), pp. 13–28
7. Delac, K., Grgic, M.: 'A survey of biometric recognition methods'. Proc. Of 46th Int. Symp. Electronics in Marine, 2004, pp. 184–193
8. Marino, C., Penedo, M.G., Penas, M., et al.: 'Personal authentication using digital retinal images', Pattern Anal. Appl., 2006, 9, pp. 21–33
9. Jain, A., Hong, L., Pankanti, S.: 'Biometric identification', Commun. ACM, 2000, 43, (2), pp. 91–98
10. Das, R.: 'Retinal recognition - biometrics technology in practice', J. Doc. Identity, 2007, 22, pp. 11–14
11. Abrmoff, M.D., Garvin, M.K., Sonka, M.: 'Retinal imaging and image analysis', IEEE Trans. Med. Imaging, 2010, 3, p. 169208
12. Womack, M.: 'The eyes have it', Sens. Rev., 1994, 14, (4), pp. 15–16
13. Usher, D., Tosa, Y., Friedman, M.: 'Ocular biometrics: Simultaneous captureand analysis of the retina and iris' (Springer, 2008), pp. 1–23
14. Sabaghi, M., Hadianamrei, S.R., Zahedi, A., et al.: 'A new partitioningmethod in frequency analysis of the retinal images for human identification',J. Signal Inf. Process., 2011, 2, pp. 274–278
15. Choras, R.S.: 'Personal identification using retina', J. Med. Inform. Technol.,2009, 13/2009, pp. 53–58
16. Harris, A.J., Yen, D.C.: 'Biometric authentication: assuring access toinformation', Inf. Manag. Comput. Secur., 2002, 10, (1), pp. 12–19
17. Marino, C., Penedo, M.G., Penas, M.: 'Retinal based authentication viadistributed web application'. EUROCAST 2005, 2005 (LNCS, 3643), pp.386–391
18. Ortega, M., Penedo, M.G., Rouco, J., et al.: 'Personal verification based onextraction and characterisation of retinal feature points', J. Vis. Lang.Comput., 2009, 20, pp. 80–90
19. Lajevardi, S.M., Arakala, A., Davis, S.A., et al.: 'Retina verification systembased on biometric graph matching', IEEE Trans. Image Process., 2013, 22, (9), pp. 3625–3635
20. Saraswathi, K., Jayaram, B., Balasubramanian, R.: 'Retinal biometrics based authentication and key exchange system', Int. J. Comput. Appl., 2011, 9, (1), pp. 1–7
21. Chen, L., Zhang, X.-L.: 'Feature based retinal image registration', Matlab Central, last accessed on 19 December, 2013, 2009, http://www.mathworks.com.au/matlabcentral/fileexchange/23015-feature-basedretinal- image-registration
22. Bevilacqua, V., Cambo, S., Cariello, L., et al.: 'A combined method to detect retinal fundus features'. Proc. of European Conf. on Emergent Aspects inClinical Data Analysis, 2005, pp. 1–6
23. Pabitha, M., Latha, L.: 'Efficient approach for retinal biometric template security and person authentication using noninvertible constructions', Int. J. Comput. Appl., 2013, 69, (4), pp. 28–34
24. Ahmed, M.I., Amin, M.A., Poon, B., et al.: 'Retina based biometric authentication using phase congruency', Int. J. Mach. Learn. Cybern., 2013, 5, (6), pg. 933–945, doi: 10.1007/s13042-013-0179-z
25. Oinonen, H., Forsvik, H., Ruusuvuori, P., et al.: 'Identity verification based on vessel matching from fundus images'. Proc. of 2010 IEEE 17th Int. Conf.on Image Processing, 2010, pp. 4089–4092
26. Hisham Al-Assam, Rasber Rashid and Sabah Jassim, "Combining Steganography and Biometric Cryptosystems for Secure Mutual Authentication and Key Exchange" , The 8th International Conference on Internet Technology and Secured Transactions, pp.369-374 , 2013.
27. Y.J. Chin, T.S. Ong, A.B.J. Teoh, K.O.M.Goh, "Integrated biometrics template protection technique based on fingerprint and palm print feature-level fusion", Elseiver Journal- "Information Fusion 18", pp.161-174 , 2013.
28. E. Cauich, R. Gómez, R. Watanabe, "Data Hiding in Identification and Offset IP Fields", Proceedings of 5th International School and Symposium of Advanced Distributed Systems (ISSADS) 2005,LNCS vol. 3563, (Springer, Berlin, Heidelberg, 2005) pp. 118–125.
29. M.Vatsa, R.Singh, and A.Noore, "Improving biometric recognition accuracy and robustness using dwt and svm watermarking," IEICE Electronics Express, vol.2, pp. 362-367, Dec. 2005.
30. Alauddin Bhuiyan , Akter Hussain, Ajmal Mian, Tien Y. Wong, Kotagiri Ramamohanarao, Yogesan Kanagasingam "Biometric authentication system using retinal vessel pattern and geometric hashing", IET journal, 2018
31. Kasturba Medical College Manipal
32. HiriyannaG., S., G. R. Manjula and Niharika. "Image Steganography in Yuv Color Space." (2017).
33. Womack, M.: 'The eyes have it', Sens. Rev., 1994, 14, (4), pp. 15–16
34. Kanagasingam, Y., Bhuiyan, A., Abrmoff, M.D., et al.: 'Progress on retinal
35. image analysis for age related macular degeneration', Prog. Retin. Eye Res., 2013, 38, pp. 20–42

AUTHORS PROFILE

Mr.Krishnaraj Chadaga M Tech student, Department of Computer Science & Engineering Manipal. Institute of Technology, Manipal - Karnataka. He obtained his B.E. degree from SMVITM, Bantakal affiliated to VTU Belgaum, Pursuing M.Tech in Computer Science Engineering from Department of Computer Science and Engineering, Manipal Institute of Technology, Manipal. He has worked on IOT as a part of B.E. project. "Features of RSA SecurID Access: is his current ongoing MTech project. . Areas of interest include Artificial Intelligence , Machine learning, Big data Analytics, Information security etc.

Ms. Musica Supriya, Assistant Professor, Department of Computer Science & Engineering Manipal. Institute of Technology, Manipal - Karnataka. She obtained her B.E. degree from SMVITM, Bantakal affiliated to VTU Belgaum, M.Tech in Software Engineering from Department of Information and Communication Technology, Manipal Institute of Technology, Manipal. She has worked on NS2 to simulate black hole and gray hole attacks in Mobile Ad-hoc Networks as a part of B.E. project. "Multi-Modality Face Recognition: An Information Theoretic Approach" is a publication as part of her research thesis of MTech. Mini-projects were carried out on crop-soil suitability analysis using ontology. Areas of interest include Data mining, Image processing, Social Network Analysis and Natural language processing.

Dr. Srikanth Prabhu, Member IEEE, Member ACM, has completed his schooling from Delhi Public School , Bhilai, in 1993. He then went on to do his Master of Science in Mathematics (Major) and Specialization in Computer Science, from Sri Sathya Sai Institute of higher Learning, Deemed University, Prashantinilayam, Puttaparthy, Andhara Pradesh, in 1998. He then went on to complete his Master of Technology in Computer Science and Data Processing, in 2003, from Indian Institute of Technology, Kharagpur. He then completed his Ph.d in Retinal Biometric Pattern Analysis System, in 2013, from Indian Institute of Technology, Kharagpur. He has published numerous papers in international and national journals and international and national conferences. He has won many awards at national and international level, significant one's are, Best Project Award, for M.tech Thesis, titled 'Face Recognition System for Criminal Identification using Distributed Computing' at IIT , Kharagpur and Best Paper Award at FTMS , Malaysia.