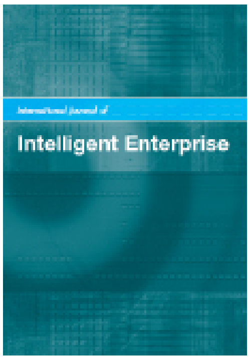


International Journal of Intelligent Enterprise

ISSN online: 1745-3240 - ISSN print: 1745-3232
https://www.inderscience.com/ijie

Fusion of multimodal biometric authentication using gradient pyramid, PCA and DWT

R. Devi, P. Sujatha

DOI: 10.1504/IJIE.2021.10035656

Article History:

Received:	07 February 2019
Last revised:	25 August 2019
Accepted:	17 February 2020
Published online:	30 November 2022

Fusion of multimodal biometric authentication using gradient pyramid, PCA and DWT

R. Devi* and P. Sujatha

Vels Institute of Science Technology and Advanced Studies (VISTAS),
Chennai, India
Email: newdevi21@gmail.com
Email: sujinagi@gmail.com
*Corresponding author

Abstract: Authentication and identification is the most challenging task in our daily life. Biometric system provides an automatic identification of an individual using his/her behavioural or physiological traits. In this work, multimodal biometric traits namely fingerprint and iris, have been used. These traits were pre-processed using Wiener filter and applying some morphological operations. The pre-processed biometric traits were segmented and fused using three algorithms namely discrete wavelet transform (DWT), principal component analysis (PCA) and gradient pyramid (GP). The fused biometric traits using GP provides a better result without losing the meaningful information. The feature extraction and classification were carried out using grey scale co-occurrence matrices (GLCM) and support vector machine (SVM). Authentication using fused biometric traits gives accuracy as 83.75, whereas the accuracy using fingerprint 73.75% and iris was 78.48%.

Keywords: biometric authentication; gradient pyramid; support vector machine; SVM; discrete wavelet transformation; DWT; principal component analysis; PCA; iris and fingerprint; fusion.

Reference to this paper should be made as follows: Devi, R. and Sujatha, P. (2023) 'Fusion of multimodal biometric authentication using gradient pyramid, PCA and DWT', *Int. J. Intelligent Enterprise*, Vol. 10, No. 1, pp.73–98.

Biographical notes: R. Devi is working as an Assistant Professor in the Department of Information Technology, School of Computing Sciences, Vels Institute of Science and Technology, Chennai. She has 14 years of teaching experience in both UG and PG Level. She has produced six MPhil scholars. She has published 25 research papers in various international journals in which nine are Scopus indexed journals. She has presented 18 papers in various international conferences and 15 papers in national conferences. She serves as an editorial board member/reviewer of various reputed journals. Her research interests include image processing and data mining.

P. Sujatha is working as a Professor in the Department of Information Technology, School of Computing Sciences, Vels Institute of Science and Technology, Chennai. She has 21 years of teaching experience in both UG and PG Level. She has produced five PhD scholars and seven MPhil scholars. Currently, she is guiding her eight PhD scholars in Vels Institute of Science and Technology. She has published 48 research papers in various international journals in which 16 are scopus indexed journals. She has presented 25 papers in various international conferences and 21 papers in national conferences. She serves as an editorial board member/reviewer of various reputed journals. She has conferred a special recognition under 'Excellence Teaching in Higher

Education' for the futuristic and outstanding best practices in the field of Education from various organisations. She is also a member in CSI-Chennai Chapter. Her research interests include image processing, network security and data mining.

1 Introduction

Within recent years, verification becomes an important issue in current society. The most popular application in today's life style link with the transaction relates with the financial sector takes place in ATMs, e-commerce etc., (Azzin et al., 2008). The important phenomena such as that the person can prove their own claims. The system with computer may helpful in identifying a person using the number of techniques and procedure required to identify the person.

The ability, presentation and dependability depend on the technologies with the biometric. The achievement for biometric modality varies from the efficiency of the technology. The implementation focuses solution for the total security comprises of the biometric system as a part. A next generation focuses on the market involving the biometric. The user attenuation increases the receipt and also the demand for the biometric. The easy user direction makes it more dependable. The technology improvement will cover the biometric needs. The important growth in various fields such as the biometric modalities and also the multimodal biometrics (Ross and Jain, 2006).

The important growth in various fields such as the bio metric modalities and also the multimodal biometrics (Ross and Jain, 2006). The factors such as the inconsistency with internal noise class, quality way of data, non-universality and extra factor may affect the sensitivity of uni-modal biometric systems for the applications in the real world. The effect to improve the presentation of the individual matchers in the effective side. An importance for security in multimodal biometric systems, which may guarantee the users with genuine to access the system. The result is to enhance the presentation of the individual matchers in effective side. An importance of security in multimodal biometric systems may be to guarantee the users with genuine to access the system. The traits based on the biometric facing many problems, some of them related with the technology itself. The enrolment problems occurred with the non-universal biometric traits, inadequate correctness can causes data acquisition for certain environment. The measurement relates the biometric, which can inherently naturally varied in the environment of the existence of background noise, distortion due to the signal and the features relates the biometric signal features and the environmental variations. Classification based on the biometric trait, can efficiently strong. The effect of spoofing can be limited. These problems can be overcome by the use of multi biometrics. Monwar et al. (Conti Militello et al., 2010) proposed integration based on the rank level fusion. The fusion scheme combines the information from the various fields. The special qualities such as the starting from the utilising procedure such as the principal component analysis and the Fisher's linear discriminant methods. The fusion scheme combines the information from the various fields and special qualities such as procedure utilisation which includes the principal component analysis and the Fisher's linear discriminant methods. The both the method focused on the character matchers (facial features, ear sensitivity and autograph) can individuality authenticate using the development of multimodal biometric system. The novel can utilise the fusion based on the rank level, which can join the outcome from unlike biometric matchers. The peak rank can combined the matchers using the peak rank, logistic failure and large count etc. The result shows the fusion of modalities, which can improve the biometric systems. The systems also include the low quality data. Ross et al. (Gayathri and Ramamoorthy et al., 2012) talked about the element level. The level pursues

1 for face – combination of PCA and LDA co-effective and the LDA coefficients relating the R, G and B channels

2 the element level with combination parts, for example, face and hand modalities.

The highlight in the pros and cons for fusion to this level. The motivation relates the work, which shows the availability in the fusion can emphasise the requirement of further research. Chong et al. (2006) introduced the detailing for the biometrics essentially the concealment for arbitrary portion. The channel utilises the property of the iris pictures which incorporate least normal relationship vitality (MACE) channel with iris verification. The prepared pictures were duplicated utilising the irregular part in recurrence space for bio measurements acknowledgment for their iris validation. The biometric layout can give issues of examination. The proposed technique can ready to diminish the computational load, for the decrease in size. The problems with biometric security, including fingerprint ID. Biometrics are certainly superior to anything passwords with regards to security, however they are not idiot proof. Welcome to the universe of biometric validation, where your eyes, ears, and fingerprints are the entrance code to demonstrate singular character. This paper defeats the biometric distinguishing proof is an innovation that recognises and confirms people dependent on physical qualities. A biometric ID framework incorporates unique mark distinguishing proof, iris and retina, facial acknowledgment, stride, or voice. The biometrics market is developing as the innovation is being hailed as the new age of resistance for law implementation against programmers. Section 2 depicts Literature survey, Section 3 talks about existing methods including the proposed technique. Section 4 talks about the results and discussion following by conclusion as an end.

2 Literature survey

Aboshosha et al. (2015) proposed the synthesis in the finger print, iris and the face traits. The traits use the score level, which can improve the system performance such as the accuracy. The classifiers outputs are treated as score, which can be classified as the normalised in the first step using the min-max normalisation. The rules of the fusion were sum, product and the weighted sum need for the fusion. The experimental result shows the multimodal biometric systems which can out perform the uni-modal biometric systems. The rule such as the weighted sum was the best results in the comparing with the sum or the product method.

Abdolahi et al. (2013) proposed the multimodal system for the biometric system fusion for the iris and the fingerprint were proposed. The level for the decision in the fusion and the bio metric results are weighted in participation to become last choice. The fluffy rationale is another parameter for the impact of biometric outcome blend. The proposed technique can achieves the high precision with looking at of uni-modal frameworks.

Günlü et al. (2018) proposed an irregular coding plan that comprises of superposition of a rate-mutilation code for imparting the activity grouping and a layered coding with binning for mystery key age. The opposite depends on standard properties of entropy capacities. The mystery key and protection spillage rate limits have similar articulations, and the new capacity rate bound is the entirety of the mystery key and capacity rate limits of the produced mystery model for a shrouded source.

Nguyen and Dang et al. (2018) proposed structure is not just safe against assaults on the system yet additionally secures biometric formats put away in the untrusted server's database, because of the mix of fluffy responsibility convention and non-invertible change strategies. The remarkable element when contrasted with past biometric based remote validation structure is its capacity to safeguard the touchy information against various types of insider assaults. The server's chairman is unequipped for using data spared in its database to imitate the customers and hoodwink the entire framework in light of the fact that protected registering in the server is ensured by utilising a safe coprocessor implanted in the server. Furthermore, the framework execution is kept up with the help of irregular orthonormal venture, which diminishes computational unpredictability while safeguarding its exactness.

Merhav (2018) proposed an approved client demands confirmation, guaranteeing his/her way of life as one of the supporters, he/she needs to give a biometric signal once more, and afterward the framework, which recovers additionally the partner message of the asserted endorser, creates a gauge of the mystery key, that is at last contrasted with the mystery key of the asserted client. If there should be an occurrence of a match, the validation solicitation is affirmed, else, it is rejected.

The security of a secret word plan is needy upon the capacity to keep passwords mystery. Thusly, a dialog of expanding secret phrase security should start with the undertaking of picking a secret phrase. A secret phrase ought to be picked with the end goal that it is anything but difficult to recollect, yet hard to figure. There are a couple of ways to deal with speculating passwords which we will examine, alongside strategies for countering these assaults (Ueda, 2003). Confirmation is the initial phase in access control, and there are three normal components utilised for verification: something you know, something you have, and something you are. This article gives you great comprehension of the three components of confirmation and how they can be utilised together with multifaceted verification. The next session discusses about the working procedure for the existing method.

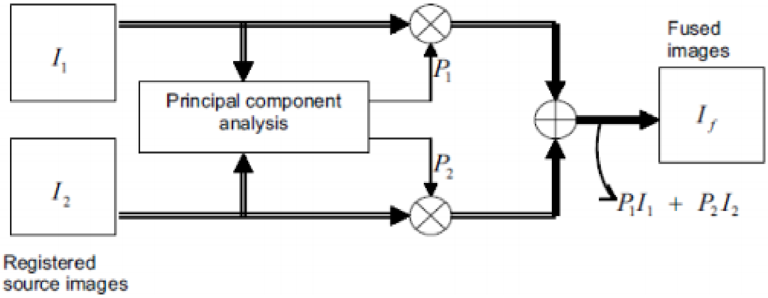
3 Existing methods

3.1 Principal component analysis

PCA is one kind of convert for the vector space, which can be reduced for the multidimensional data set. The data sets can be lower dimensions for the analysis of PCA transform. The transform perform based on the number of correlated variables into uncorrelated variables called principal components. The advantage of PCA, where the data size compression is required for the dimensions, can be altered. Because of the compression much loss of information can be predetermined at the output image. The process of fusion can be accomplished using the weighted average of images to be fused. The eigenvector can relate the largest eigenvalues for the covariance matrices for the each resource, which can be obtain the weights for the each source of image.

The information can be a flow diagram for PCA-based image fusion algorithm can be shown below. The input image can be fused I1 (x, y) and I2 (x, y). The arrangement of two column vectors with the empirical means was subtracted. The resulting vector can have the dimension of nX2, in this n represent the length of each image vector. The computation of individual eigenvector and the eigenvalues which can results in vector were computed. The eigenvectors can corresponds to the larger eigenvalues can be obtain. The normalised components P1 and P2 (i.e., P1 + p2 = 1). The computed results can obtain the eigenvector. The fused image can be represented.

Figure 1 The technique for image fusion using PCA



Notes: If (x, y) = P1I1 (x, y) + P2 I2 (x, y) (1).

Figure 2 Image level fusion using PCA (see online version for colours)

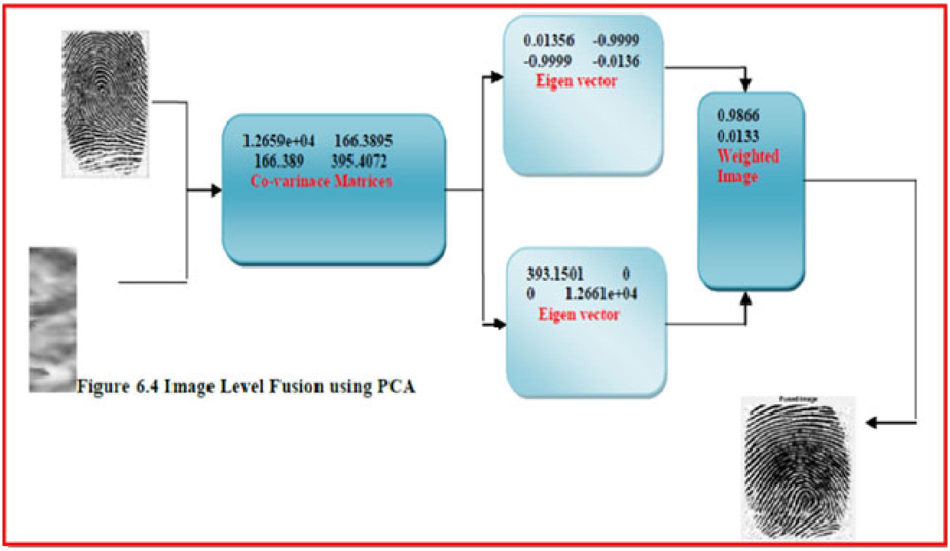


Figure 1 shows general method of principal method analysis, in which the image I1 and another part I2 under goes the PCA. P1 and P2 give as an input to the mixer P1 and P2. The output is combined using the adder block (P1I1 + P2I2) and given as the fused images (Thai and Tam, 2010).

The stepwise procedure for fusing fingerprint and iris using PCA algorithm depicted in Figure 2.

The stepwise description of the PCA algorithm is given below

Step 1 The column vectors (image matrices) are generated for both the input images, i.e., fingerprint and iris.

Step 2 The mean for each column is calculated which is subtracted from each column. The column vectors form a matrix X.

Step 3 The covariance matrix of the two column vectors formed in step 1 is calculated.

$$\begin{pmatrix} 1.2659\mathrm{e}+04 & 166.3895 \\ 166.389 & 395.4072 \end{pmatrix}$$

Step 4 The diagonal elements of the 2 × 2 covariance vector would contain the variance of each column vector with itself, respectively.

Step 5 The eigenvalues and the eigenvectors of the covariance matrix are computed. The eigenvalue of the fingerprint is given below.

$$\begin{pmatrix} 0.01356 & \rightarrow & -0.9999 \\ -0.9999 & \rightarrow & -0.0136 \end{pmatrix}$$

The eigenvalue of the iris is given below.

$$\begin{pmatrix} 393.1501 & \rightarrow & 0 \\ 0 & & 1.2661\mathrm{e}+04 \end{pmatrix}$$

Step 6 The column vector corresponding to the larger eigenvalue is normalised by dividing each element with the mean of the eigenvector. T is the eigenvector corresponding to the largest eigenvalues of the images A and B, the weight values of image A and image B is as follows:

$$\begin{pmatrix} 0.9866 \\ 0.0133 \end{pmatrix}$$

Step 7 The components of the normalised eigenvector act as the weight values that are respectively multiplied with each pixel of the two input images.

Step 8 The sum of the two scaled matrices calculated in step 6 will be the fused image matrix.

Then, the fusion is accomplished using a weighted average as where I_f is the fused image and I_A and I_B represent images A and B respectively. Figure 3 shows the fused image using PCA technique.

Figure 3 Fused image using PCA

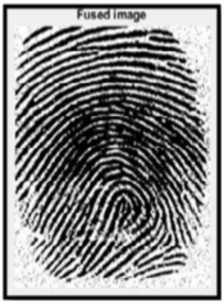


Table 1 Fused multimodal biometric the using the PCA technique

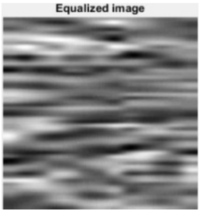
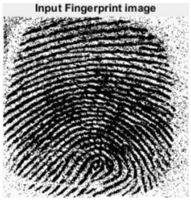
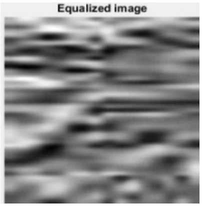
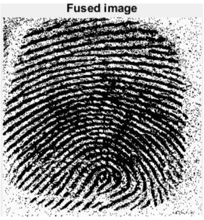
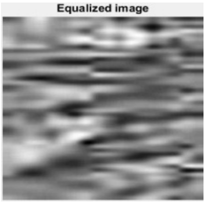
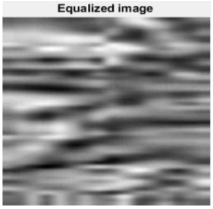
S. no	*Fingerprint*	*Iris*	*Fused template*
1			
2			
3			
4			

Table 1 Fused multimodal biometric the using the PCA technique (continued)

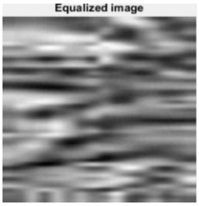
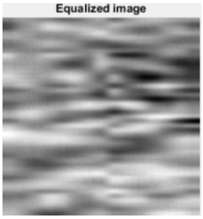
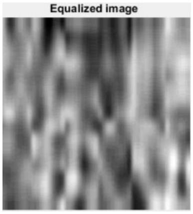
S. no	*Fingerprint*	*Iris*	*Fused template*
5			
6			
7			

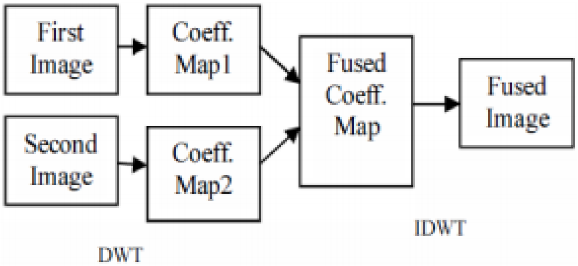
Table 1 consists of an enhanced fingerprint, resized iris and the resultant fused template using the PCA technique.

3.2 Discrete wavelet transformation

The discrete wavelet transformation (DWT) can covers the picture from the spatial area to recurrence space. The picture can be isolated utilising the vertical and level lines. The lines spoke to as the primary request of DWT; the picture can be isolated with four sections, for example, the LL1, LH1, HL1 and HH1. The four sections spoke to the four frequencies for the territories in the pictures. The low recurrence space LL1 is more delicate with human eyes. The insight about the recurrence areas LH1, HL1 and HH1 characterised as more detail. The wavelet change can play out the principal wellspring of pictures, which can create a combination include delineate on principles set. The wavelet coefficients in the fusion technique can map for the source of images. This technique helps in the fusion decision map. Finally the result of inverse wavelet transform is the fused image.

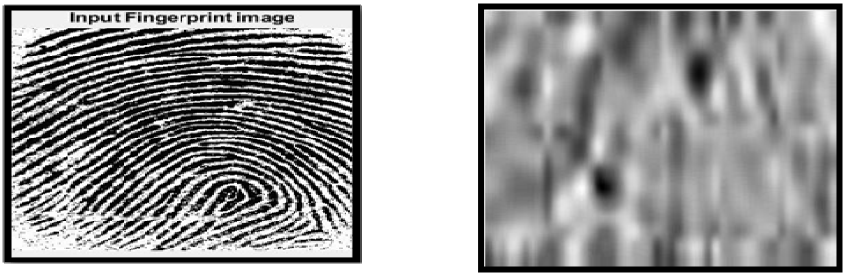
Figure 4 shows the discrete wavelet transforms done in the first stage. The first image and second image taken for the analysis. In the first image the coefficient of Map1 and the coefficient of map 2 were combined to form the fused coefficient map. The fused image composed of fused coefficient drawn from the IDWT.

Figure 4 Image fusion using DWT



The first step is to acquire the two images to be fused. The next step is to resize both the images into the same size and apply a DWT to those images. DWT transform the two images into discrete wavelet coefficients. The fusion rule is applied to those wavelet coefficients. Figure 5 shows the input images which are enhanced fingerprint and the resized iris.

Figure 5 Input images for fusion using DWT



The stepwise procedure for fusing fingerprint and iris using DWT algorithm depicted in Figure 6.

Figure 6 Fingerprint and iris Fusion using DWT (see online version for colours)

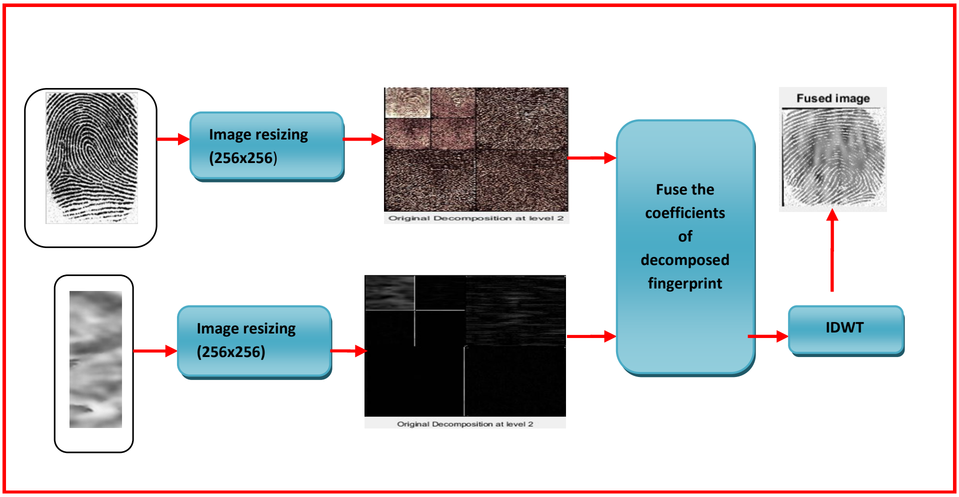


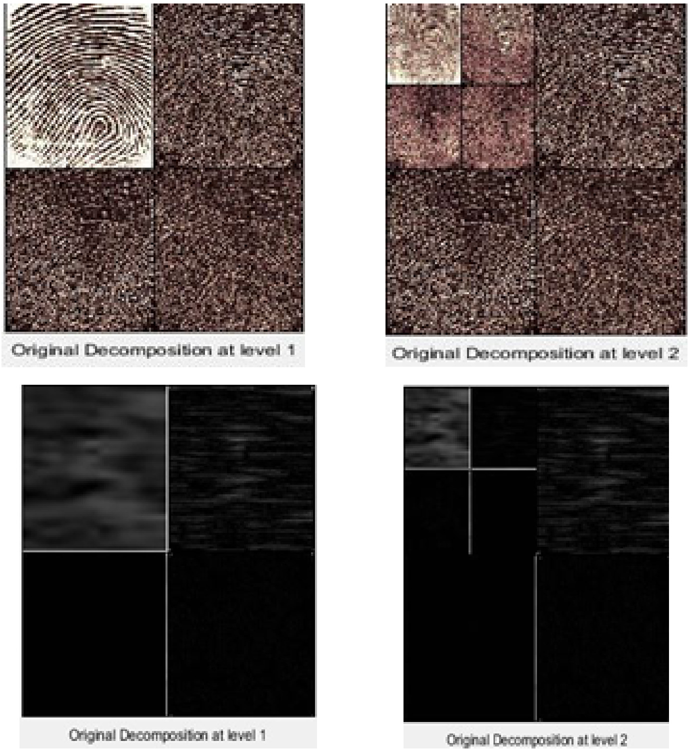
Image resizing (256x256)
Original Decomposition at level 2
Image resizing (256x256)
Original Decomposition at level 2
Fuse the coefficients of decomposed fingerprint
IDWT
Fused image

The stepwise description of the DWT algorithm is given below.

Step 1 The two input images, i.e., enhanced fingerprint and iris are resized for fusion.

Step 2 The resized fingerprint and iris undergoes two-level decomposition. The DWT decomposition consists of a chain of high pass and low pass filters. The output of the single-level decomposition consists of four sub-images having the size equal to half size of the original image. Hence, HH1, HL1, LH1, LL1 are sub-bands manipulated from a single level decomposition of images. Figure 7 shows the two-level decomposition of fingerprint and iris.

Figure 7 Two-level decomposition of fingerprint and iris (see online version for colours)


Original Decomposition at level 1
Original Decomposition at level 2
Original Decomposition at level 1
Original Decomposition at level 2

Step 3 It means that the low-pass filter is applied and followed by high pass filter. The second level wavelet decomposition specified with the lowpass and high pass decomposition filters for the low pass decomposition (LoD) and the high pass decomposition filters for the low pass decomposition (LoD) and the highpass decomposition (HiD). HL image contains the vertical detail coefficients; HH contains the diagonal detail coefficients. Here, the decomposition is manipulated for two levels. The next level of decomposition is performed using only the LL image. The result is the next four sub-band images HH2, HL2, LH2, LL2 and each of size equal to half the LL image size.

Step 4 The coefficients of the decomposed images are finally fused using MAX fusion technique.

Step 5 Finally, inverse DWT is performed to get the fused image.

Figure 8 provides the fused template using DWT technique.

Figure 8 Fused image using DWT

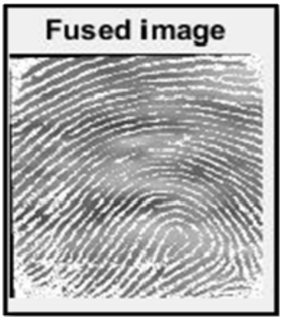


Table 2 consists of an enhanced fingerprint, resized iris and the resultant fused template using DWT technique.

Table 2 Fused multimodal biometric using DWT technique

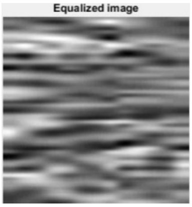
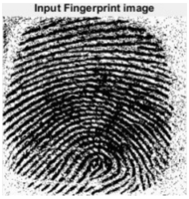
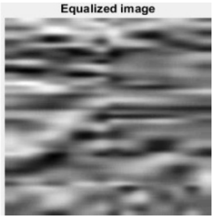
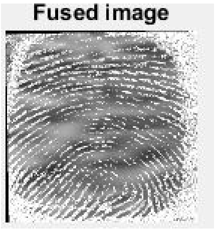
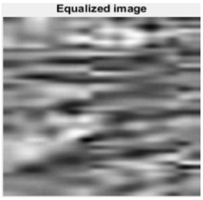
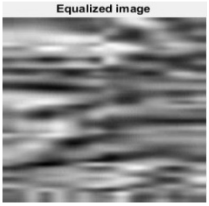
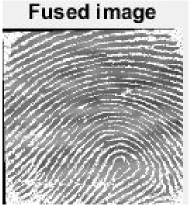
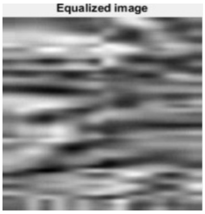
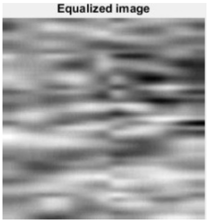
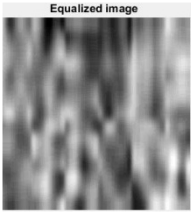
S. no	*Fingerprint*	*Iris*	*Fused template*
1			
2			
3			

Table 2 Fused multimodal biometric using DWT technique (continued)

S. no	*Fingerprint*	*Iris*	*Fused template*
4			
5			
6			
7			

The wavelet-based approach is more appropriate for performing fusion tasks for the following reasons,

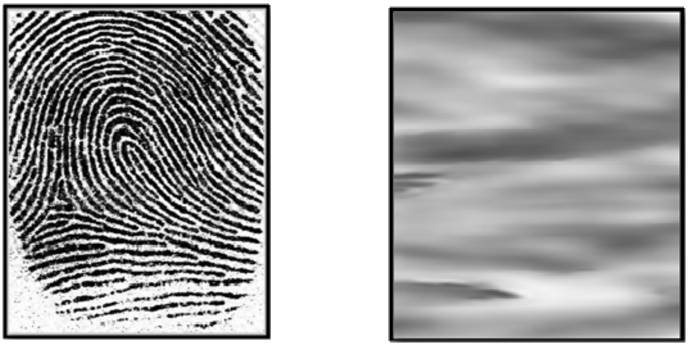
- It is a multi-scale (multi-resolution) approach well suited to manage the different image resolutions. DWT is used in some image processing applications including image fusion.
- The discrete wavelets transform (DWT) allows the image decomposition in different kinds of coefficients preserving the image information.

3.3 Image fusion using GP method

A new proposed authentication based on the biometric, which approaches the biometric images such as iris and fingerprint. The fusion techniques use the fingerprint and iris images and also the gradient pyramid (GP) approach, which mutual to shape a lone image. The image fusion algorithm works on the GP such as the multi-resolution, multi-scale decomposition algorithms. The several step processes are involved in the decomposition section. The first step is the decomposition of original image into GP. The four directions of the each layer have been fully decomposed in to gradient decomposition. The evaluation of the fusion effect was based on the entropy value, average gradient method, mean and standard deviation value of the process.

Image fusion algorithm based on GP is one of the multi-scale, multi-resolution decomposition algorithms. Original input images are decomposed into Gauss pyramid, after that, gradient decomposition was completed on each layer in four directions and the fusion effect is evaluated using possible fusion metrics. In the algorithm, the input images fingerprint and iris are decomposed. Figure 9 is stated for decomposition.

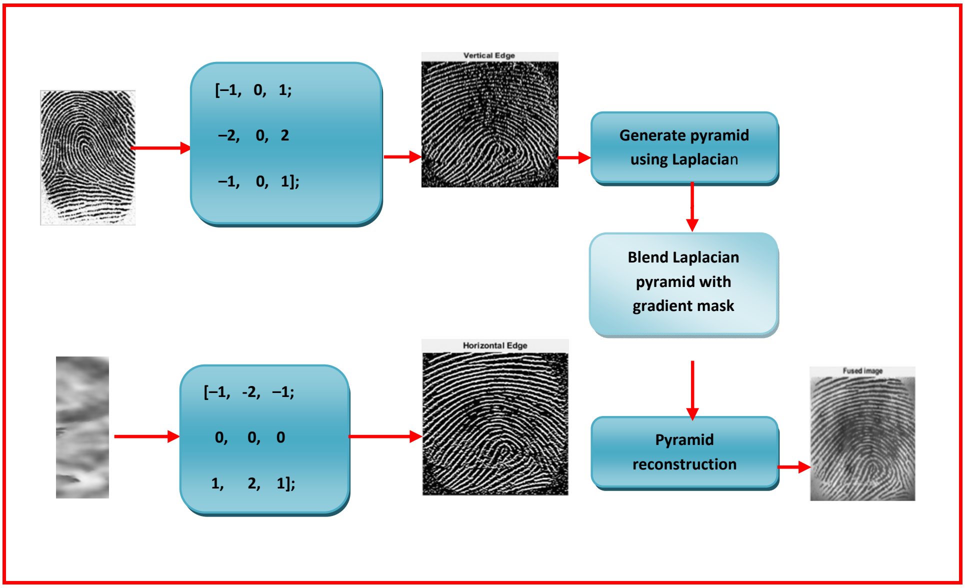
Figure 9 Input images for fusion using GP



The preprocessing step starts with the input acquired images. The features of the images are extracted for the process of exercise and testing images. The matching images find the comparison stuck between features set.

The stepwise procedure for fusing fingerprint and iris using DWT algorithm depicted in Figure 10.

Figure 10 Image level fusion using GP (see online version for colours)



In the field of digital image processing, multi-resolution pyramid is the main form of multi-scale representation of images. The image is decomposed into pyramid consists of two steps: image smoothening and image sampling. Gauss pyramid decomposition as follows,

$$G_{1(i,j)=\sum_{m=-2}^{2}\sum_{n=-2}^{2}\omega(m,n)} G_{l-1(2i+m,2j+n)} (1 \le 1 \le N, 0 \le i \le R1, 0 \le j \le Ci) \tag{6.2}$$

In equation (6.2), *G* represents the original image, *G* as the zero layers of Gauss pyramid, The stepwise description of the GP algorithm is given below.

Step 1 The two input images, fingerprint and iris passed through Gauss low-pass filter and downsampling, the first layer of Gauss pyramid was received; and then the first layer would be passed through Gauss low-pass filter and downsampling, the second layer of Gauss pyramid was received.

Step 2 After each layer of pyramid decomposition, the GP image undergoes gradient filter.

Step 3 The gradient filter operator consist of four decomposition level namely the detailed information on horizontal, vertical and two diagonal directions. Then the decomposition obtained as

$$D_{LK} = d_{k*(G_L + \omega_0 \cdot G_L)} \quad 0 < L < N \quad K = 1,2,3,4 \tag{6.3}$$

In the above equation (6.3),

D_{LK}	the GP decomposition of the *L* layer in the *k* direction
G_L	the *L* layer image of Gauss pyramid.
d_k	the filter operator of the *k* direction, defined as follows.

The fused template using GP is shown in Figure 11.

Figure 11 Fused template using GP

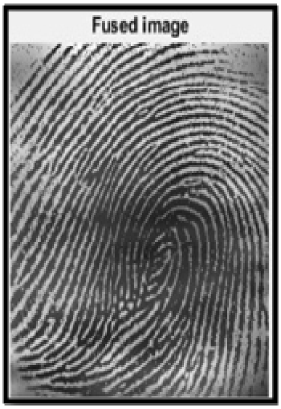
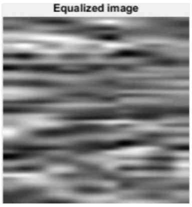
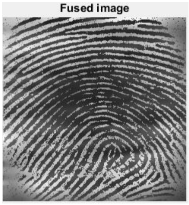
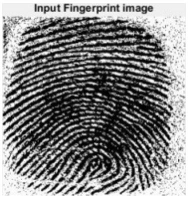
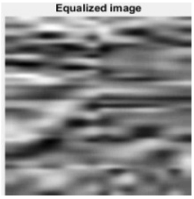
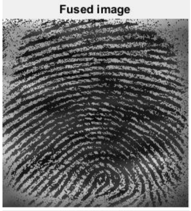
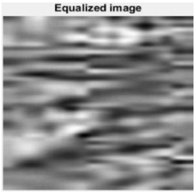
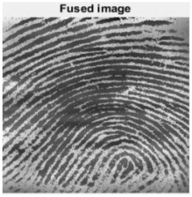
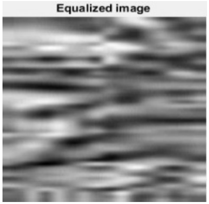
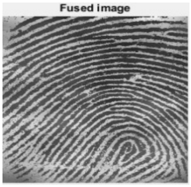
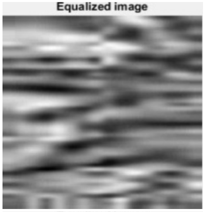
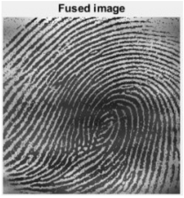
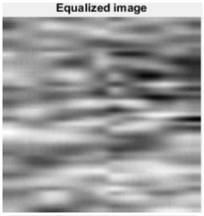
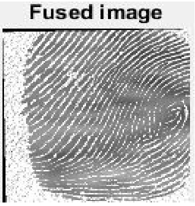
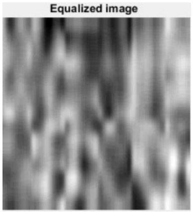
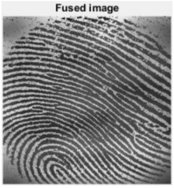


Table 3 consists of an enhanced fingerprint, resized iris and the resultant fused template using the GP technique.

Table 3 Fused multimodal biometric using GP technique

S. no	*Fingerprint*	*Iris*	*Fused template*
1			
2			
3			
4			
5			
6			
7			

3.4 Sift feature extraction

The four basic steps present in the SIFT algorithm. The difference of Gaussian (DoG) is the first stage to estimate a scale space extrema. The second one will be the localisation key point, here key points for the candidates are localised and the low level contrast points are eliminated for the process. The third level focused on the key point orientation assignment helps in local image gradient. The generator for descriptor in computing the local level image descriptors. The local level descriptors obtained using key points extracted from the image gradient magnitude and orientation. The proposed model uses the two biometrics traits such as the fingerprint and iris. The process performed individually on these two biometrics. The method uses the GP fusion technique to take authentication decision in the level of high or low.

1. The preprocessing steps are fist performed on fingerprint image. The next level continues with the normalisation; remove noise, binarisation and thinning. The process continues with the SIFT algorithm on the image. The image processed with the computer version able to detect and describe the images with the local features. The features extracted based on the GLCM algorithm. The next level fingerprint image goes to the fusion process.
2. The features obtained from the fingerprint, which leads to the matching process performed using the support vector machine (SVM) classifier. The classifier of the SVM type helps in identifying the input fingerprint image is genuine or not. The result shows the matched one indicates the user can be authenticated.
3. The iris image can be checked using the above two process.
4. The GP method performs the biometric fusion. Then fused image follows the step 1 and step 2.

Figure 12 Block diagram of proposed method

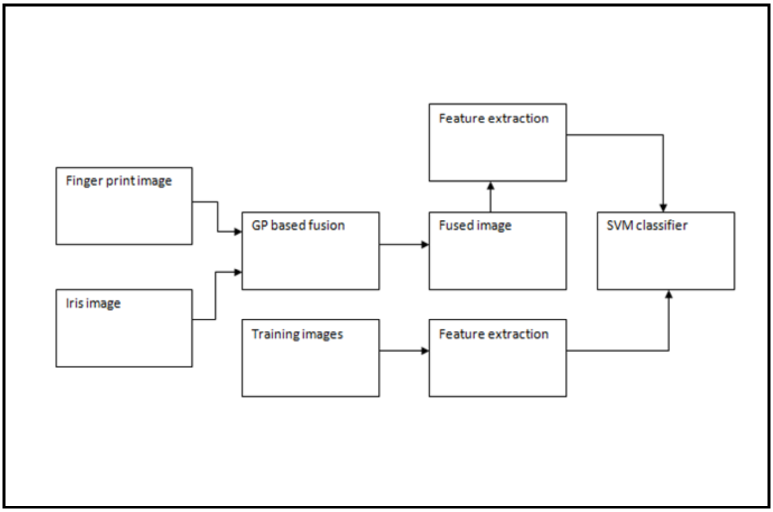


Figure 12 shows a processing of two images the first one is finger print image, the next one iris image. These finger images undergoes the GP based fusion techniques, which has the fused image with the feature extraction block, the block provides the extraction of useful information of the block. The SVM classifies the features extracted for the training images. The SVM classifier blocks classify the test images and the trained images.

4 Results and discussion

4.1 Performance of fusion algorithms

Image level fusion of fingerprint and iris is being carried out using three fusion algorithms namely PCA, DWT, and GP. The performance analysis of these algorithms is measured by calculating some image quality metrics.

Table 4 Performance matrices using GP, DWT and PCA based fusion

Performance matrices	*GP*	*PCA*	*DWT*
PSNR	89	88	50
Standard deviation	40	110	43
NAE	0.8	0.02	2
MSE	0.1	0.14	1.9
SSIM	0.02	0.99	0.03
Normalised cross correlation	0.03	0.01	0.023
Xydeas and Petrovic metric	0.8	0.7	0.024
cross entropy	0.01	0.02	0.11

Table 4 shows the result values for the GP, PCA and DWT methods. The values are list in the table. The tabulation values based on the performance metrics the GP reaches the highest values. The PSNR the GP attains the maximum value 89 compared with the PCA and DWT. The standard deviation maximum value 110 obtained by PCA method, medium value obtained by the DWT method, the lowest value is 40 achieved by the GP. The NAE, PCA values reaches the minimum value of 0.02, the GP reaches the 0.8 and the 2 for DWT. The minimum mean square error (MSE) reaches the minimum value of 0.1 in GP, maximum value of 0.14 and finally reaches the 1.9 for the DWT. The SSIM achieves the higher value of 0.99 for PCA, the DWT value of 0.03. The normalised cross correlation of PCA is 0.01, DWT is 0.023 and the 0.03 for the GP method. The Xydeas and Petrovic metric achieved the PCA for 0.7, the GP for 0.8 and 0.024 for the DWT. Finally the cross entropy reaches the GP values for the 0.01, the method PCA reaches for the 0.02 and the DWT for the 0.11.

Table 4 gives the experimental results of the performance analysis of the three fusion techniques PCA, DWT, and GP. From Table 4 fusion of enhanced fingerprint and iris using GP algorithm provides a better fusion image by retaining the information when compared with the other two algorithms. The analysis has been graphically represented using ROC curve.

Figure 13 shows a PSNR comparison for the different methods of GP, PCA and DWT. The PSNR comparison in which the GP reaches the range of 80 to 83 compared with the other method of PCA and DWT. Figure 14 shows an input images with the NAE here the GP reaches the moderate values between the PCA and DWT.

Figure 13 PSNR comparison (see online version for colours)

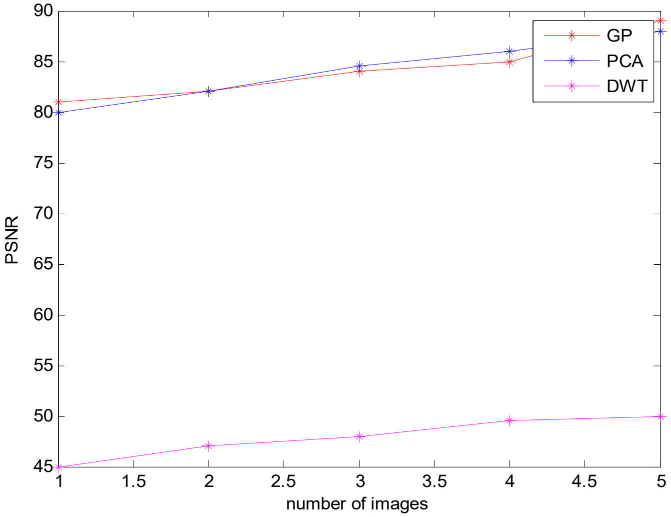


Figure 14 Standard deviation comparison (see online version for colours)

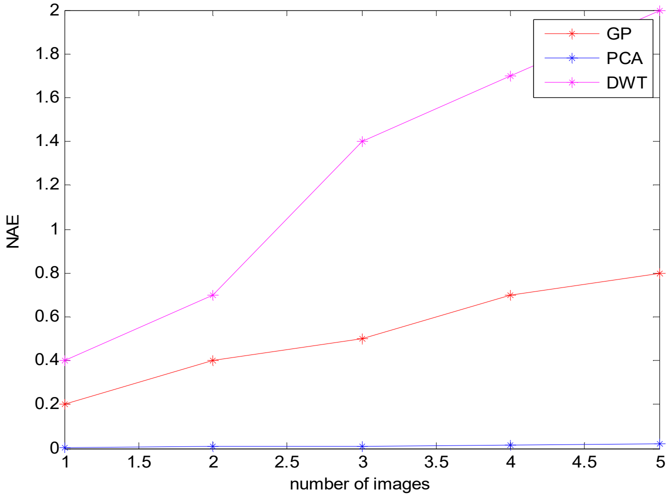


Figure 15 shows an NAE comparison graph between the GP, PCA, and DWT for the standard deviation, the GP lies lower than the PCA and DWT. Figure 16 shows an MSE comparison for the three methods here also GP lies lower than the PCA and DWT.

Figure 15 NAE comparison (see online version for colours)

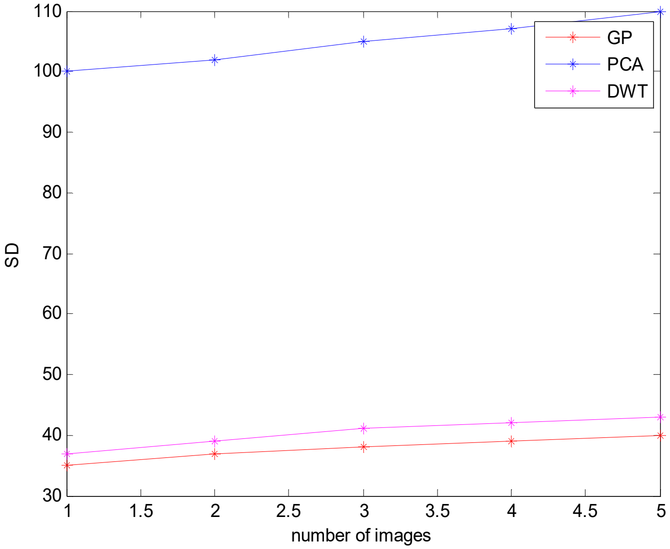


Figure 16 MSE comparison (see online version for colours)

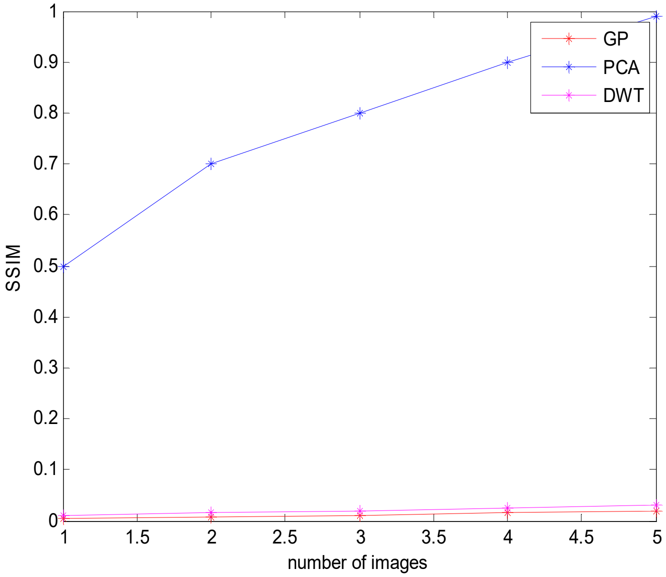


Figure 17 SSIM comparison for the number of images with the MSE, here the GP lies lower than the PCA and DWT. Figure 18 shows an NC values for the number of images GP, PCA and the DWT. In NCC, GP shows a number of images with NCC with the higher values.

Figure 17 SSIM comparisons (see online version for colours)

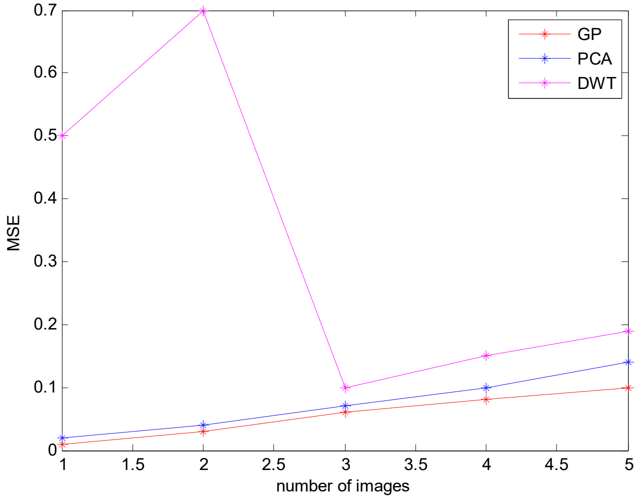


Figure18 NCC comparisons (see online version for colours)

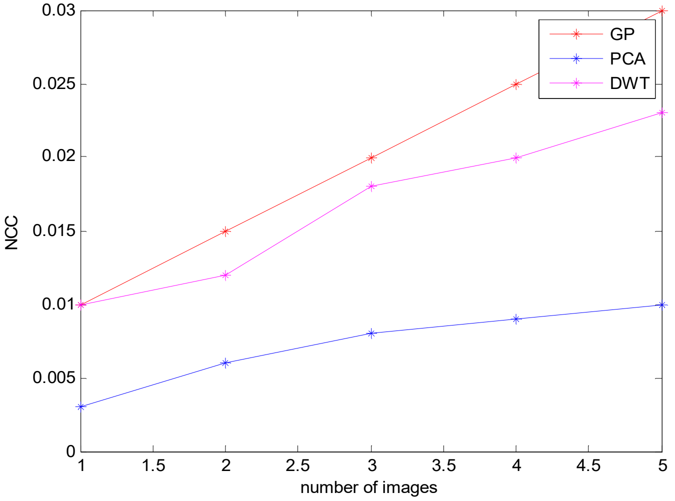


Figure 19 shows comparison metrics for the GP, PCA and DWT. The GP lies between the PCA and DWT. The GP lies in the range of the 0 to 5. Figure 20 shows the number of images and the cross entropy here the GP reaches 0 to 0.01value. The GP reaches the very small values for the 0.06 to 5 values.

Figure 19 Xydeas and Petrovic metric comparison (see online version for colours)

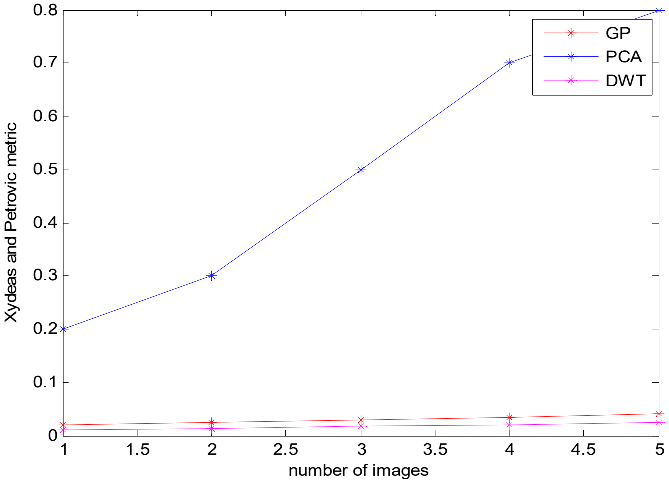
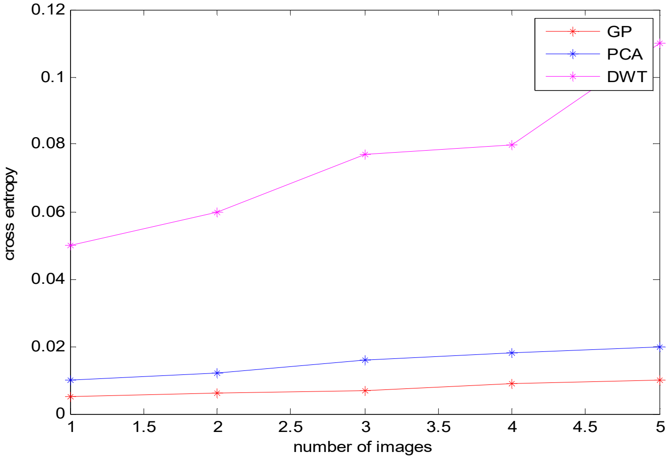


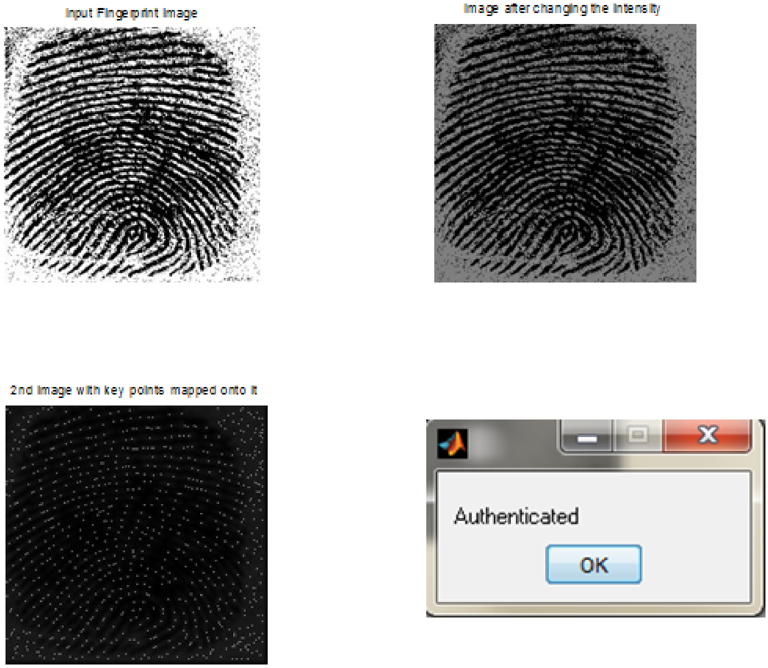
Figure 20 Cross entropy comparison (see online version for colours)



4.2 Performance of an accuracy of biometric authentication system by uni-modal and Multi-modal traits using SIFT and SVM

Figure 21 shows the finger print method using the authentication with the SIFT key with the point features. Figure 22 shows that the iris authentication with its SIFT key points features. Figure 23 shows the GP based fused image authentication with its SIFT key point features. Table 4 shows the GP, DWT and PCA based fused images performance results. The GP based fusion gives the better result for comparing the DWT and PCA. The PCA based fusion can gives the fair result as same as GP method.

Figure 21 Simulated result of Fingerprint authentication (see online version for colours)


Input Fingerprint Image
Image after changing the Intensity
2nd Image with key points mapped onto it
OK

Authenticated

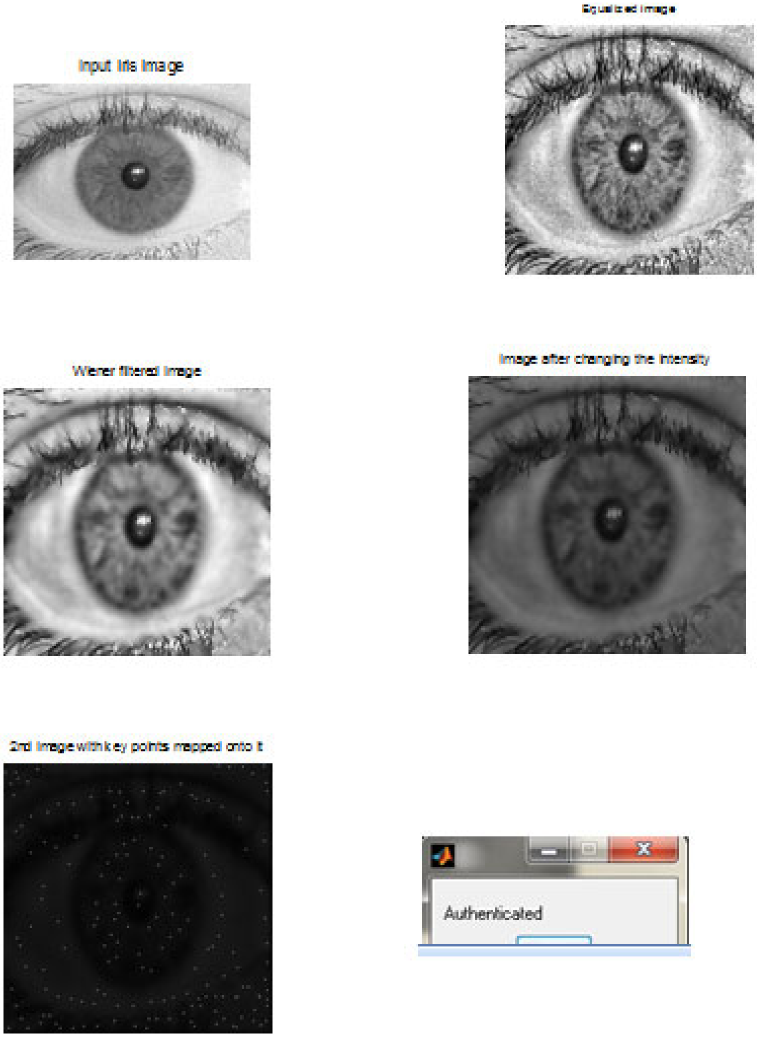
Figure 21 shows a result of the proposed input images such as the figure of an input figure print image, figure of input image after changing the intensity, the figure of second image with key points mapped on it, the figure of shows authenticated image. The figure shows the changing of the input finger print image, after the changing the intensity the image changes to the intensity of the key points. Finally the input image is authenticated in the processes.

Figure 22 shows the figure of input iris image, figure of equalised image, figure of Wiener filter image, figure of image after changing the intensity, figure of 2nd image with points mapped onto it. The figure shows authenticated images, image preprocessing such as the equalisation, filtering processes using the Wiener filtering and the image enhancement processes.

The simulation results for the iris authentication shown in Figure 2.

Figure 23 shows an combined image of figure of vertical edge, figure of horizontal edge, figure of fused image, figure of image after changing the intensity, figure of 2nd key points mapped onto it, the figure of authenticated image. The image processing such as the vertical edge, horizontal edge, fused image, image after changing the intensity and the second level transformation of intensity of the image. Finally the analysis result shows the authentication of image.

Figure 22 Simulated results of iris authentication (see online version for colours)



Input Iris Image
Equalized image
Wiener filtered image
Image after changing the intensity
2nd image with key points mapped onto it

Authenticated

Figure 23 Simulated results of fused image authentication (see online version for colours)

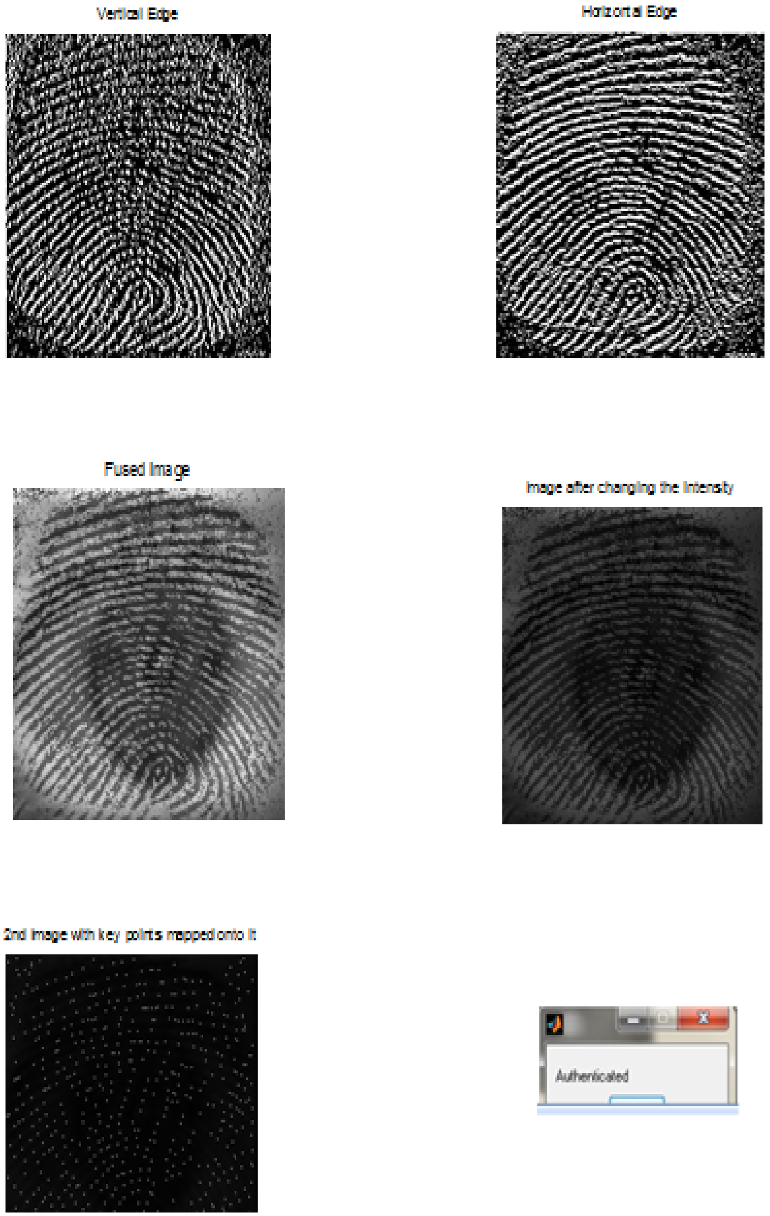

Vertical Edge
Horizontal Edge
Fused Image
Image after changing the Intensity
2nd image with key points mapped onto it
Authenticated

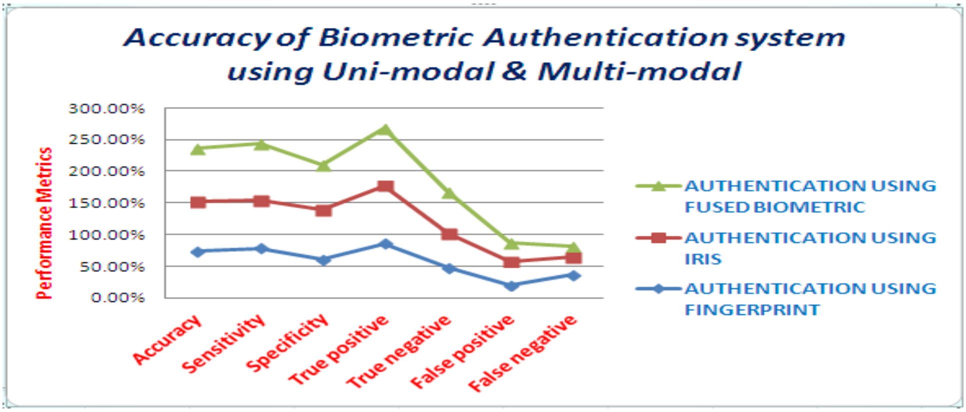
Table 5 shows the accuracy parameters for the authentication system. The table clearly shows that authentication the system using multimodal biometrics gives more accuracy than authenticating the system using uni-modal. The above measures prove that authenticating the system by fusing the two biometrics such as fingerprint and iris provides a best accuracy than authenticating using fingerprint and iris separately.

Table 5 Accuracy parameters for authenticating a uni-modal biometric vs. multimodal biometrics

Sl. no.	*Measures*	*Accuracy*	*Sensitivity*	*Specificity*	*True positive*	*True negative*	*False positive*	*False negative*
1	Fingerprint	73.75%	78.33%	60.00%	85.45%	48.00%	19.53%	36.11%
	Iris	78.48%	76.67%	80.00%	92.00%	53.33%	38.33%	29.17%
	Fused image	83.75%	88.33%	70.00%	89.83%	66.67%	29.44%	16.67%

The accuracy of multimodal biometric authentication system is also depicted using the graph given in Figure 24.

Figure 24 Accuracy of biometric system authentication (see online version for colours)



5 Conclusions

The paper discussed about the fusion of multi-modal biometric traits namely fingerprint and iris. The fusion of multimodal-biometric really improves the reliability for the biometric system requires for the sensitive verification and validation. In the proposed system, the fusion of the enhanced fingerprint and the segmented iris was carried out using three existing fusion algorithms namely PCA, DWT and GP. By analysing image quality metrics such as Xydeas and Petrovic, entropy, MSE, NCC, PSNR, NAE, etc., GP gives a better fusion image without degrading the image quality. The fused image was trained and tested by extracting the key points using SIFT and also authenticated using SVM. The paper mainly deals with biometric authentication system. It provides a reliable accuracy using multimodal biometric traits, i.e., by combining fingerprint and iris when compared with uni-modal biometric, i.e., authenticating fingerprint and iris separately.

References

Abdolahi, M., Mohamadi, M. and Jafari, M. (2013) 'Multimodal biometric system fusion using fingerprint and iris with fuzzy logic', *International Journal of Soft Computing and Engineering*, Vol. 2, No. 6, pp.504–510.

Aboshosha, A., Dahshan, K. and Kara, E.A. (2015) 'Score level fusion for fingerprint, iris and face biometrics', *International Journal of Computer Applications*, February, Vol. 111, No. 4, pp.47–55.

Azzin, A., Marrara, S., Sassi, R. and Scotti, F. (2008) *A Fuzzy Approach to Multimodal Biometric Continuous Authentication*, June, Vol. 7, pp.243–256, Springer Science, Fuzzy Optim Decis Making.

Chong, S.C., Teoh, A.B.T. and Ngo, D.C.L. (2006) *Iris Authentication Using Privatized Advanced Correlation Filter in ICB*, pp.382–388.

Conti Militello, S. and Vitabile, S. (2010) 'A frequency-based approach for features fusion in fingerprint and iris multimodal biometric identification systems', *IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews*, Vol. 40, No. 4, pp.384–395.

Gayathri, R. and Ramamoorthy, P. (2012) 'A fingerprint and palmprint recognition approach based on multiple feature extraction', *European Journal of Scientific Research*, pp.514–526.

Günlü, O., Kittichokechai, K., Schaefer, G.C. (2018) 'Controllable identifier measurements for private authentication with secret keys', *IEEE Transactions on Information Forensics and Security*, DOI 10.1109/TIFS.2018.2806937.

Jagadeesan, A. (2010) 'Secured cryptographic key generation from multimodal biometrics: feature level fusion of fingerprint and iris', *Arxiv Preprint arXiv: 1003.1458*, Vol. 7, No. 2, p.2837.

Jagadeesan, A. (2011) 'Protected bio-cryptography key invention from multimodal modalities: feature level fusion of fingerprint and iris', *European Journal of Scientific Research*, Vol. 49, No. 4, p.484502.

Lakshmi, A.J. and Ramesh, I. (2012) 'PKI key generation using multimodal biometrics fusion of fingerprint and iris', *Matrix*, No. 2, p.285290.

Merhav, N. (2018) 'Ensemble performance of biometric authentication systems based on secret key generation', *IEEE Transactions on Information Theory*, DOI 10.1109/TIT.2018.2873132.

Nguyen, T.A.T. and Dang, T.K. (2018) 'Privacy preserving biometric-based remote authentication with secure processing unit on untrusted server', *IET Biometrics*, Vol. 8, No. 1, pp.79–91.

Ross, N. and Jain, A.K. (2006) *Handbook of Multibiometrics*, 1st ed., Number ISBN-13: 978-0-387-22296-7, Springer-Verlag.

Shukla, N. (2010) 'Invariant features comparison in hidden markov model and sift for offline handwritten signature database', *International Journal of Computer Applications*, Vol. 2, No. 7, pp.0975–8887.

Teoh, C. and Ngo D.C.L. (2006) 'Iris authentication using privatized advanced correlation filter in ICB', *ICB 2006: Advances in Biometrics*, pp.382–388.

Thai, L.H. and Tam, H.N. (2010) 'Fingerprint recognition using standardized fingerprint model', *IJCSI International Journal of Computer Science Issues*, May, Vol. 7, No. 3, p.7.

Ueda, K. (2003) 'Investigation of off-line Japanese signature verification using a pattern matching', *Proc. of the 7th ICDAR*.