Finger Feature based Biometric Steganography Method for Secure Authentication

[1]Aditi Sharma,[2]V.R.Singh
[1,2]Department of Electronics and Communication, Faculty of Engineering & Technology, Mewar University, Rajasthan

Abstract : The biometric steganography methods are able to improve the data security for biometric verification. In this paper, a feature adaptive method is provided for improving the biometric authentication and communication. The work is specifically about to hide the fingerprint feature in facial image and perform the authentication on receiver side after retrieval. The proposed model is defined in three mains stages. In first stage, the facial cover image is processed by generating multiple agents. Each agent analyzed the coverage region based on frequency strength and identify the effective cover region. In second stage, the mathematical filters are applied on fingerprint image to generate the features. In this stage, the sequence based mapping is applied to hide the features within the cover facial region. In final stage, the image features are reterived at the receiver side and performed the authentication over the dataset. The method is applied on a sample of 10 images. The results identified the effective data hiding with significant MSE, PSNR and SSIM values.

IndexTerms **- Biometric Authentication, fingerprint, face, steganography, data security.**

I. INTRODUCTION

The communication of sensitive information in public domain is always a challenge. Different data hiding[1][2], encoding[16] and authentication[17][18][19] based methods were suggested by the researchers to improve the data security. Steganography[1][2][3][4][5] is one such approach in which the sensitive information or secret message are hide in some other message, media or carrier. This carrier can be of same or different form. In digital world, this carrier can be email, audio, image, video etc. The basic architecture of steganography is shown in figure 1.

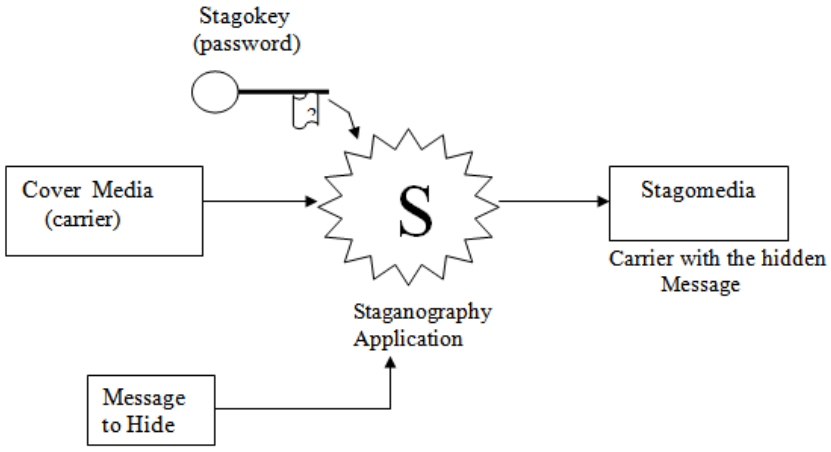

Figure 1 : Basic Steganography Model

Figure 1 has shown the basic steganography model in which steganography method is applied to some application or communication model. The input to this application is the cover media and the secret message. The stegokey is defined to define the method to perform data hiding. The steganography method actually use this stegokey to hide the message within the cover media at the source or sender end. Once the steganography is performed, the stegomedia file is generated. This file contains the hidden secret message within the communication media file. This file can be distributed over the public domain. Once the stegofile is received at the receiver end, the reverse operation is performed by using stegokey to recover the secret message.

The accuracy and reliability of steganography method depends on the difficulty level to extract the message from the stegomedia file without using the secret key or stegokey. Various methods[4][6][7][8][9] were proposed by the researchers to improve the data security. The steganography methods depends on the applications, domains and the mediafile involve as the secret file as well as cover file. In this paper, one of such effective steganography method is proposed called biometric steganography. In this method, one biometric image is hide within other biometric image to improve the biometric[18][19][20] authentication.

The paper has proposed a three stage model to improve the effectiveness and reliability of biometric steganography. In this section, the basic concept of steganography is discussed by exploring the overall functioning of steganography process. In section II, the work provided by earlier researchers is presented and discussed. In section III, the proposed model is described with relative description. In section IV, the results obtained from the proposed model for sample images are discussed. In section V, the conclusion of work is presented.

II. RELATED WORK

The steganography methods were defined by the researchers to provide the salutation to various issues of data hiding. The optimization was achieved for improving the data hiding capacity and to improve the data security. In this section, the work defined by the earlier researchers is discussed and presented. Author[1] has used the spatial information to hide the information. The high intensity edge region was identified based on textural analysis. Once the region is identified, the edge magnitude parameter was used to perform data hiding within the high resolution images. Author[2]has proposed the DWT based data hiding method to improve the data security. The n-level based decomposition method was defined in this work to generate the effective region. The sub-band based evaluation was defined to perform data hiding within the image. The frequency component based analysis was performed to store the information within image and to improve effectiveness of data hiding. Author[3] has used the modified logistic chaotic map to perform data hiding in color images. The domain transformation based wavelet decomposition was defined to improve the capacity and security of data hiding method. The key space and bifurcation approach was defined to ensure the better data security in the images. Various tests were conducted to perform data security and safety. Author[4] has used the histogram based method as a generalization approach to perform bit specific data hiding. The DCT coefficient and histogram analysis were combined to hide the data within color images. The metrics based evaluation was also performed to identify the distortion and to perform pixel specific data storage within the extracted region. The tracing method was also defined to maintain the visual quality and to improve the quality of data hiding.

Author[5] has proposed a hybrid model using fuzzy and neural based methods to improve the data hiding in images. The analysis on the pixel intensity was performed to avoid the data degradation and to perform effective data hiding. The three-bits were processed in this work for data hiding to improve the capacity of data hiding and to maintain the quality of cover image. Author[6] has applied the modulus function to perform data hiding within images. The method maintains the quality of steganography image and to improve the capacity of cover image. The image component based analysis was performed by the author to analyze the color component of images. Author[7] has defined wavelet transformation and QR factorization based approach to generate the cover region over the image. The energy distribution and pixel variation based analysis was defined to generate the pattern over the image and to perform data hiding. The computational complexity and singular value decomposition method was defined to perform data hiding in images. The color extracted region was processed on multiple bands to factorize the image and to improve the capacity and robustness of data hiding. Author[8] has defined a Fresnelet transformation based frequency coding measure to perform data hiding in image. The frequency subband based feature analysis was defined to improve the data secrecy. The visual structure and scrambling analysis based approach to improve the data security in images. Author[9] has defined the wavelet fusion based approach to achieve robustness of data hiding against attacks and eavesdropping. The spatial information based method was defined to generate the effective region on cover image. The color layer based method was defined to improve the data hiding within images. Author[10] has proposed the interpolation based reversible steganography method to improve data hiding against different distortions. The method improves the payload to improve the quality and capacity of data hiding. The neighbor pixel based evaluation method was defined to reduce the complexity of data hiding process and to maintain the quality of the image. The interpolation based method was defined to generate the neighbor difference analysis and to improve data security in images.

Author[11] has defined the biometric data hiding within the image by using reinforcement approach. The computational complexity based method was defined to reduce the storage space and to improve the visual quality of image. The local features of facial image were generated to hide the fingerprint information. The method provides the effective information hiding while maintaining the visual quality of image. Author[12] has defined a data hiding based biomodel biometric process to improve the image authentication. The independent component analysis based evaluation was defined to generate the effective region. The method was applied on fingerprint and iris biometric to improve the data hiding. Author used the modulation and quantization to achieve the effective multi model authentication. Author[13] has used the PSO (Particle Swarm Optimization) based method to extract the region from image and to improve the biometric authentication. The demographic method was defined to extract the cover pattern on face image and to hide the fingerprint image within the generated region. The visual perception of biometric image was improved by the author. Author[14] has analyzed the skin tone of images to improve the data hiding of within the image. The color space based analysis was defined to extract the effective region and to improve the data hiding. The feature evaluation method was defined to improve the data security and capacity for images. Author[15] has used the template based biometric data hiding for images. The diffusion based data hiding method was used to generate the chaotic sequence and to perform pixel based data hiding. The change evaluation was defined to improve data security in images.

III. RESEARCH METHODOLOGY

The secure data communication in public domain is the essential environment for any application. Such network suffers from intruders and attackers. The steganography method provides the secure way to communicate the sensitive information or authentication specification through such shared medium. The user level and password specific information can be hiding behind an image for secure transmission of information. The situation becomes more critical when the biometric authentication is performed and some image authentication information is communicated. Such biometric images are having the important and high resolution information that can provide the authentication to any online or offline system. The fingerprint or iris based authentication systems are available to provide secure communication over the public network. Communicating such high resolution images through unsafe medium can increase the chances of illegal access to the sensitive user information. In this research, an effective biometric information communication method is provided by hiding the biometric information within other biometric image. In this proposed model, the effective features of fingerprint image are hide within facial image by generating the adaptive pattern over it. In this paper, the model of data hiding is presented along with the specification of process model for secure information communication and authentication. The proposed model is divided in two main work stages. In first stage, the

steganography is performed by generating the pattern region over the facial image and then hide the fingerprint features within the image. The steganography stage defined in this model is shown in figure 2. Once the data hiding is performed, the biometric authentication is performed at the receiver end by extracting the fingerprint features of database images.

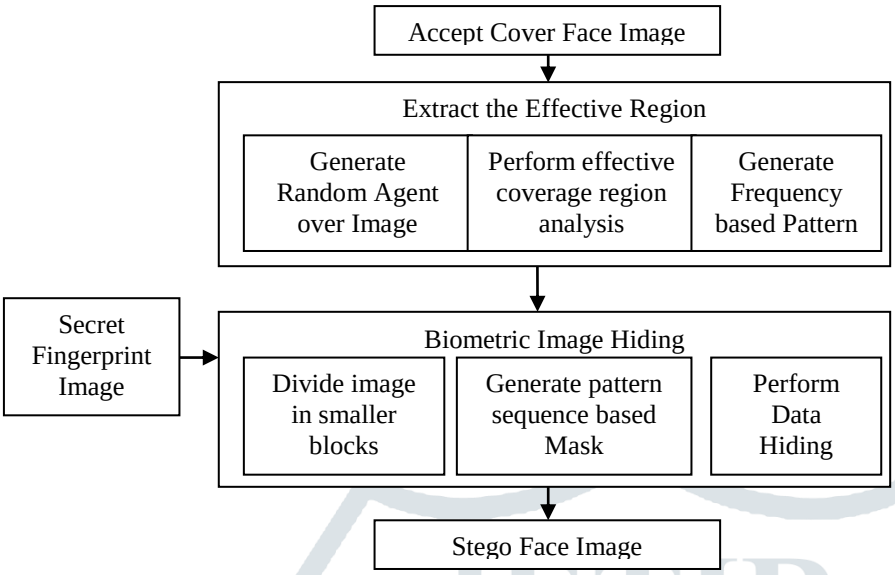

Figure 2 : Steganography Stage

Figure 2 has provided the complete description of each substage of data hiding process defined to hide the fingerprint features within the facial region pattern. The input taken to the system is the form of cover facial image and secret fingerprint image. The facial image is processed to generate the effective cover pattern over the image. To extract this cover region, the random agents are distributed over the image. These agents performed analysis within the coverage region based on frequency feature. The high frequency pixels are extracted over each region to generate the cover pattern over the facial image. Once the pattern is generated, the next work was to perform data hiding.

The fingerprint image is taken in this work as the effective data image which is required to hide within the facial pattern. The finger print is processed by the morphological operators and mathematical filters to generate the minutia points, end points and core points over the image. The featureset is generated to represent the fingerprint image distinctively. To perform the data hiding, the features is divided in the smaller blocks and the sequence mask is generated over the pattern image. Once the transformation of the feature image and cover pattern is mapped, the data hiding is performed within the image. In this stage, the fingerprint hiding is performed within the facial cover region of image.

Now this steganography image is communicated to the public medium and at the receiver end, the image is extracted and performed the feature extracted from the steganography image. The model for fingerprint authentication is shown in figure 3.

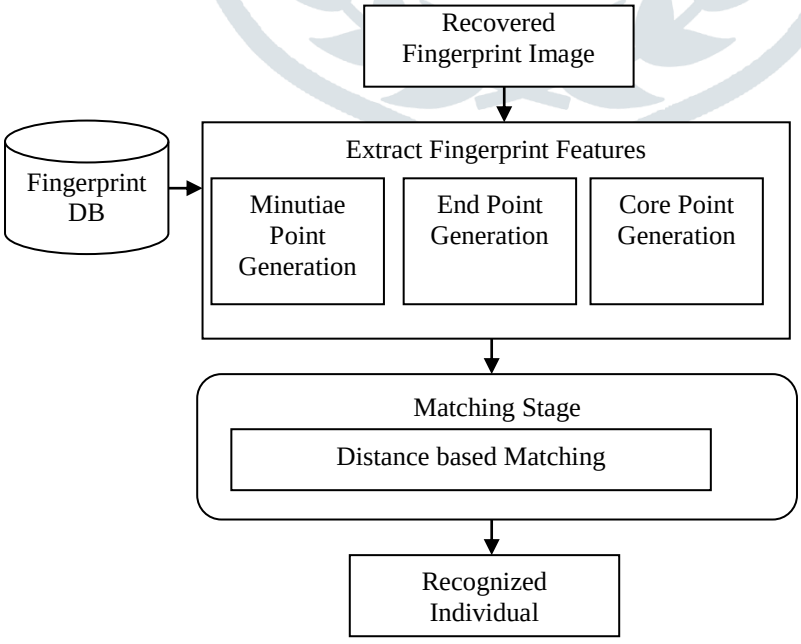

Figure 3 : Fingerprint Verification

Once the steganography image is received at the receiver side, the reverse process is performed to retrieve the fingerprint features from the facial image. The receiver side is having the fingerprint database to represent the user images. The fingerprint features

extracted from the database images in the form of minutiae point, end point and core point features. These features formed the featureset and now the extracted features are mapped to these database features. The distance based matching is applied over the fingerprint feature set to recognize the individual.
The proposed model is able to provide the secure communication of biometric high resolution images and to provide the effective authentication of fingerprint using specific feature processing. The analysis results obtained over the authenticated datasets. These results to verify the accuracy of steganography process is provided in next section.

IV. RESULTS

The proposed biometric steganography and authentication based model is applied on the larger high resolution dataset taken from external web sources. Two different datasets of fingerprint images and facial images are considered in this research. The description of fingerprint dataset is provided in table 1.

Table 1 : Features of Fingerprint Dataset

Dataset	Properties
Number of Images	337
Color	No
Lighting	Mix
Gender	Mix
Individuals	337
Resolution	296x560

The table shows that the fingerprint dataset is having high resolution images and able to define the individuals with effective fingerprint features which can identify the individual accurately. The cover facial dataset is also considered in this work for data hiding. The description of fingerprint dataset is provided in table 2.

Table 2 : Features of Face Image Dataset

Properties	Values
Database Name	UtrechtECVP
Database URL	www.pics.psych.stir.ac.uk
Number of Images	131
Color	Yes
Instances of a person	2
Viewpoint	2
Lighting	No
Resolution	900x1200
Gender	Mix
Individuals	69

Table 2 has provided the description of facial image sources and other characterization over images. Once the datasets are available, the images are transformed to the normalized form. The samplesets are generated of 10 images to perform the data hiding. The analysis is performed in terms of MSE (Mean Square Error), PSNR (Peak Signal to Noise Ratio) and SSIM (Structural Similarity) parameters. The MSE based evaluation on a sample of 10 images is provided in figure 4.

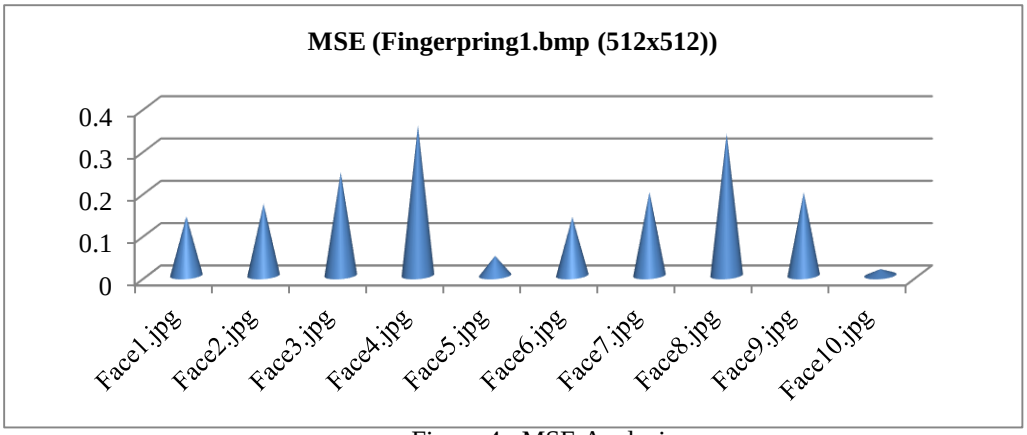

Figure 4 : MSE Analysis

Figure 4 has provided the analysis to store a fingerprint image of 512x512 in ten different facial images. The analysis is provided in terms of MSE value. In this figure, x axis represents the facial images and y axis represents the MSE value. The lesser MSE value shows more significant results. The figure shows that the maximum MSE value for any image is lesser than .33. It shows that the proposed model has achieved the significant error rate. Another analysis provided in this work is based on PSNR value and its results are shown in figure 5.

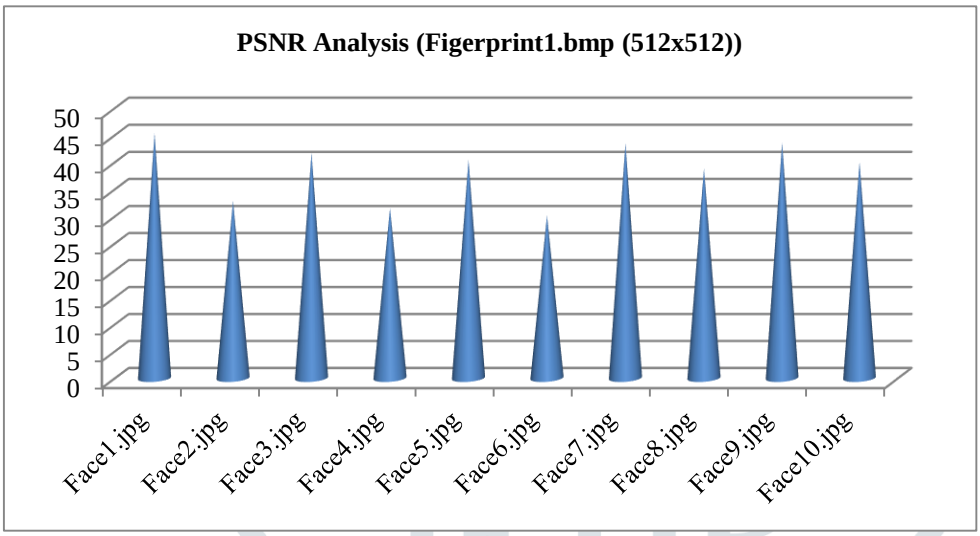

Figure 5 : PSNR Analysis (Fingerprint.bmp [512x512])

Figure 5 has provided the analysis of proposed model in term of PSNR evaluation. In this figure, x axis represents the cover facial images and the y axis represents the PSNR value analysis. The higher PSNR value verify the robustness of proposed model against noise occurrence. The figure shows that the proposed model achieved the significant PSNR value over 30 for each cover image.

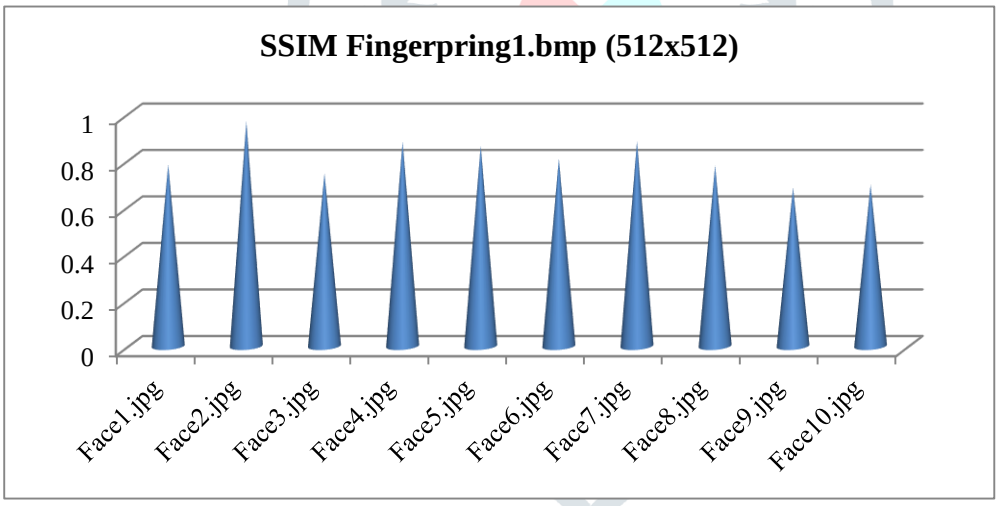

Figure 6 : SSIM Value Analysis

Figure 6 has provided the analysis of this proposed model in term of structural similarity of recovered feature image and actual image. In this figure, y axis represents the ratio of structural similarity applied on 10 dataset images. The results identified that the model has achieved the higher SSIM with value over .65. It shows that the proposed model has achieved the higher and significant results.

V. CONCLUSION

In this paper, an effective biometric data hiding and authentication model is defined. The proposed model is divided in three main stages. In first stage, the agent specific method is defined to observe the coverage region based on frequency feature analysis and to generate the cover region pattern pattern over the image. In second stage, the mathematical filters are applied to generate the fingerprint features and to hide the fingerprint based on sequence pattern within facial pattern region. In final stage, the fingerprint features are reterived at the receiver and perform the authentication. The model is applied on a sampleset of 10 images. The analysis results are generated for MSE, PSNR and SSIM parameters. The analysis results shows that the proposed model has provided effective biometric data hiding.

REFERENCES

[1] Hayat Al-Dmour, Ahmed Al-Ani, A steganography embedding method based on edge identification and XOR coding, Expert Systems with Applications, Volume 46, 2016, Pages 293-306

[2] Milad Yousefi Valandar, Peyman Ayubi, Milad Jafari Barani, A new transform domain steganography based on modified logistic chaotic map for color images, Journal of Information Security and Applications, Volume 34, 2017, Pages 142-151

[3] Della Baby, Jitha Thomas, Gisny Augustine, Elsa George, Neenu Rosia Michael, A Novel DWT Based Image Securing Method Using Steganography, Procedia Computer Science, Volume 46, 2015, Pages 612-618

[4] Kazem Qazanfari, Reza Safabakhsh, A new steganography method which preserves histogram: Generalization of LSB, Information Sciences, Volume 277, 2014, Pages 90-101,

[5] A. Saleema, T. Amarunnishad, A New Steganography Algorithm Using Hybrid Fuzzy Neural Networks, Procedia Technology, Volume 24, 2016, Pages 1566-1574

[6] V. Nagaraj, V. Vijayalakshmi, G. Zayaraz, Color Image Steganography based on Pixel Value Modification Method Using Modulus Function, IERI Procedia, Volume 4, 2013, Pages 17-24

[7] Mansi S. Subhedar, Vijay H. Mankar, Image steganography using redundant discrete wavelet transform and QR factorization, Computers & Electrical Engineering, Volume 54, 2016, Pages 406-422

[8] S. Uma Maheswari, D. Jude Hemanth, Frequency domain QR code based image steganography using Fresnelet transform, AEU - International Journal of Electronics and Communications, Volume 69, Issue 2, 2015, Pages 539-544

[9] Siraj Sidhik, S.K. Sudheer, V.P. Mahadhevan Pillai, Performance and analysis of high capacity Steganography of color images involving Wavelet Transform, Optik - International Journal for Light and Electron Optics, Volume 126, Issue 23, 2015, Pages 3755-3760

[10] Jie Hu, Tianrui Li, Reversible steganography using extended image interpolation technique, Computers & Electrical Engineering, Volume 46, 2015, Pages 447-455

[11] Lamia Rzouga Haddada, Bernadette Dorizzi, Najoua Essoukri Ben Amara, A combined watermarking approach for securing biometric data, Signal Processing: Image Communication, Volume 55, 2017, Pages 23-31

[12] Wioletta Wójtowicz, Marek R. Ogiela, Digital images authentication scheme based on bimodal biometric watermarking in an independent domain, Journal of Visual Communication and Image Representation, Volume 38, 2016, Pages 1-10

[13] Punam Bedi, Roli Bansal, Priti Sehgal, Multimodal Biometric Authentication using PSO based Watermarking, Procedia Technology, Volume 4, 2012, Pages 612-618

[14] Abbas Cheddad, Joan Condell, Kevin Curran, Paul Mc Kevitt, A skin tone detection algorithm for an adaptive approach to steganography, Signal Processing, Volume 89, Issue 12, 2009, Pages 2465-2478

[15] Gaurav Bhatnagar, Q.M. Jonathan Wu, Balasubramanian Raman, Biometric Template Security based on Watermarking, Procedia Computer Science, Volume 2, 2010, Pages 227-235

[16] **Juneja, Kapil. "An XML transformed method to improve effectiveness of graphical password authentication." Journal of King Saud University-Computer and Information Sciences (2017)**

[17] Juneja, Kapil and Chhavi Rana, “Structural and Statistical Feature processed PST for angle robust iris recognition”, International Conference on Manufacturing, Advance Computing, Renewable Energy and Communication, 2018

[18] Juneja, Kapil, and Chhavi Rana. "Multi Featured Fuzzy based Block Weight Assignment and Block Frequency Map Model for Transformation Invariant Facial Recognition." International Journal of Image, Graphics and Signal Processing 10.3 (2018)

[19] Juneja, Kapil. "Multiple feature descriptors based model for individual identification in group photos." Journal of King Saud University-Computer and Information Sciences (2017)

[20] Juneja, Kapil. "A Noise Robust VDD Composed PCA-LDA Model for Face Recognition." International Conference on Information, Communication and Computing Technology. Springer, Singapore, 2017.