PERFORMANCE ANALYSIS OF A SECURE FINGER VEIN RECOGNITION SYSTEM USING HYBRID FEATURE EXTRACTION AND FEATURE SELECTION

Satyendra Singh Thakur[1] , Dr.Rajiv Srivastava[2]

[1]Department of CSE Mewar University, Chhitorghar, Rajasthan, India

Satyendrathakur04@gmail.com

[2]Visiting faculty Mewar University, Chhitorghar, Rajasthan, India
drrajiv_sri@yahoo.com

Abstract

Most common physical biometric for authentication purposes are the fingerprint, hand, iris, face, discern vein, DNA and voice. The advantage claimed with the aid of biometric structuresis they can set up an unbreakable one-on-one correspondence amongcharacter and a bit of data. Biometrics provides authentication advantagesacross the spectrum, from IT companies to end users, and from UAID gadgetdevelopers to UAID gadget users. A good biometric is characterized with the aid of use of a characteristicit highly unique and precise:sothe possibility of any two human beings having an equivalent characteristics are going to be minimal, stable: so that the characteristicwould notchange over time, and be effortlessly acquired: as a way todelivercomfort to the user, and prevent misrepresentation of the features. Fingerprint recognition is that the oldest technique of biometric authentication. In those instances the fingerprint identitytechniquebecame used, with the name as Actyloscopy. In this work, Hybrid Feature Extraction (HFE) with security based biometric system will be introduced for evaluating the performances. HFE contains Histogram of Oriented Gradients (HOG), Stationary Wavelet Transform (SWT), Grey Level Co-occurrence Matrix (GLCM), Local Binary Pattern (LBP), and Principle Component Analysis (PCA). For Feature selection, KNN based Genetic Algorithm (GA) is used and the classifier used in this proposed methodology is error correcting code based SVM (ECOC-SVM). Finally, the performance parameters are calculated in terms of such as accuracy, precision, recall, sensitivity, specificity, false acceptance rate and false rejection rate.

Keywords:*ECOC based SVM, hybrid feature extraction, KNN based genetic algorithm, Grey Level Co-occurrence Matrix*

1. INTRODUCTION

Biometrics system is the technology of using human'sphysical as well as behavioral characters for identifying individuals. These characteristics remain unique and distinguishable [1].Behavioral biometrics includes signatures, voice recognition, gait measurement, and even keystroke recognition. Physiological biometrics includes facial recognition, fingerprinting, hand profiling, iris recognition, retinal scanning, and DNA testing [2].Each trait has its own advantages and disadvantages over others. Suitable trait is chosen depending on the type of application, its environment and various factors like uniqueness, universality, performance, acceptability etc [3]. Biometric-based identity management is increasingly being used by governments and national agencies, amongst others, for identity verification and law enforcement [4]. The biometric systems have more advantages when compared to the traditional methods such as passwords/Personal Identification Numbers (PINs). Because the passwords/PINs are easily forgettable, but the biological features are always present in the human body [5].A biometric personal verification system operates in two distinct modes: enrolment and verification. In enrolment mode, individual's biometric sample(s) are captured, processed, features extracted and labeled with the user's (client) identifier (ID). This labeled assigned feature set is called a template which is representative of the user's identity. In verification mode, claimed identity is verified by comparing the extracted features of the input/ test query to the enrolled templates [6]. Biometric systems are divided into two types such as uni-modal and multimodal biometric systems. Uni-modal biometric systems depend on a single source such as a single iris or fingerprint or palm print for authentication.A multimodal biometric system combines two or more biometric data recognition results such as a combination of a subject's fingerprint, face, iris and voice [7-8].The selection of biometric from the various biometric traits is mainly depends on the user acceptance, required level of security, accuracy, cost and implementation time [9]. Security solution are introduced to improve the authentication in the biometric systems. Because by using fake biometric information, many spoofing attacks to fool biometric systems are possible [10-11]. The challenges faced in the biometric systems are given as follows: The main drawback is that they are singly vulnerable to possible attacks, as well as little robust with respect to a number of problems. Examples are acquisition errors, possibly due to bad hardware, as well as to an actual distortion of the biometric feature (e.g. a voice altered by a cold or a dimly lit face) [12].Various distortions in the source data not only decrease the overall identification performance of a biometric system [13]. In this paper, the finger vein pattern based biometric trait is used as a authentication merit. Notwithstanding this great and increasing variety of biometrics, no biometric has yet been developed that is perfectly reliable or secure. For example, the traditional biometrics are usually frayed, forged and it is susceptible to spoofing attacks [14]. Finger-vein pattern has some advantages in uniqueness, universality, permanence and security. Hence, the finger-vein

recognition technology has been widely used in various fields, such as computer login, security inspection, ATM certification, etc [15]. The major contributions of the proposed methodology are stated as follows:

- The recognition rate of the proposed methodology is improved by two ways. First one is using various feature extraction methods such as HOG, SWT, GLCM and LBP. Here, the features from the SWT is given to the GLCM method. Second is using the feature selection method named as KNN based genetic algorithm.
- The security of the biometric system is improved by the dual RSA cryptography technique. It is used for preventing the proposed methodology from spoofing attacks.

2. LITERATURE SURVEY

Thian Song Ong *et al* [16] has introduced the Local Hybrid Binary Gradient Contour (LHBGC) and Hierarchical Local Binary Pattern (HLBP) as the texture descriptors for finger vein recognition to increase the discriminates capability of the finger vein texture. LHBGC extracts both sign and magnitude components of the finger vein image for recognition, while HLBP utilizes the LBP uniform texture pattern of the vein image without any training required. Feature level fusion integrates multiple data by using serial concatenation method. The method concatenates the multiple feature sets into a single super vector.

Abdu Gumaei*et al*[17] has presented the anti-spoof multispectral biometric cloud-based identification approach for privacy and security of cloud computing.The approach offers the solution using multi-spectral palm print as a typical biometric trait between two main phases: offline enrollment phase and online identification phase. The security is improved in this biometric system by using the RSA cryptography.

Ava Tahmasebi1 and Hossein Pourghassem [18] has introduced the game theorybased rank-level fusion of the high frequency information of ear images and combination of dynamic information of online signatures with the texture information of palmprint image. Gabor filter is used to extract locally the texture features of the ear, palmprint, and signature images. Moreover, intra-class distances are used to distinguish the genuine samples from the imposters, and also investigate the proper threshold to separate these two classes from each other.

Shan Juan Xie*et al* [19] has introduced the ensemble extreme learning machine (ELM) called the feature component-based ELMs (FC-ELMs) designed to utilize the characteristics of the features, is introduced to improve the recognition accuracy and stability and to substantially reduce the number of hidden nodes. For feature extraction, an explicit guided filter is proposed to extract the eight block-based directional features from the high-quality finger vein contours obtained from noisy, non-uniform, low-contrast finger vein images without introducing any segmentation process.

Vijay BhaskarSemwal*et al* [20] has selected the feature and identify the principle feature then we classify gait data using different machine learning technique. The different machine learning techniques are KNN, ANN, SVM, DNN and classifier fusion. Here, the analysis of variance (ANOVA) is used for feature selection and incremental feature selection (IFS) is used for selecting the features from the group of features.

3. PROPOSED METHODOLOGY

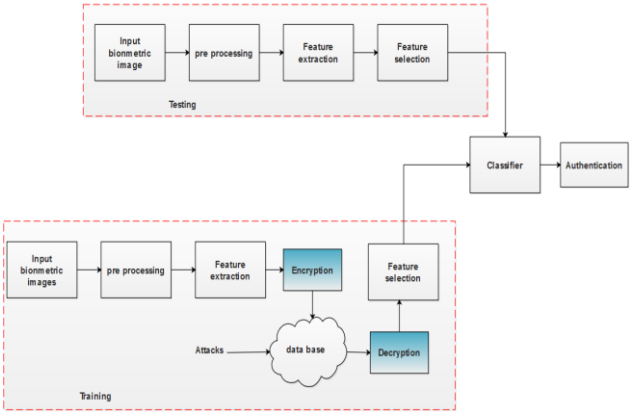

Fig.1. Block diagram of proposed method

3.1. IMAGE ACQUISITION And PRE-PROCESSING

In this proposed methodology, the finger vein images are used as the key component to access the information from the biometric systems. The sample image of the finger vein pattern is shown in the Figure 1. Then the images are preprocessed using the Gaussian filtering which is used to remove the noise from the images. The expression for Gaussian filtering is given in equation (1).

$$G(x,y) = \frac{1}{2\pi\sigma^2} e^{\frac{-x^2+y^2}{2\sigma^2}} \quad (1)$$

Where, x and y are the coordinates of the images and σ is the standard deviation.

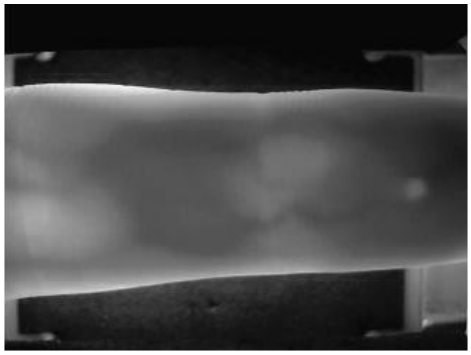

Figure 2.a. Input image

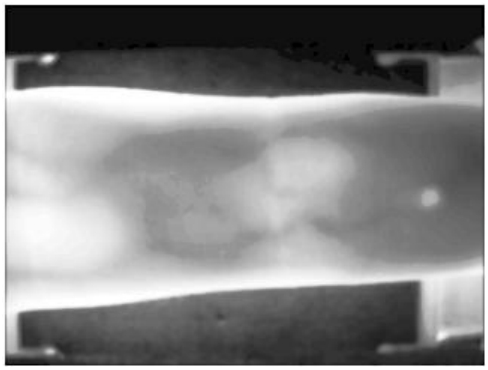

Figure2. b. Preprocessed image

3.2. HYBRID FEATURE EXTRACTION

There different kind of feature extraction technologies are used such as HOG, SWT, GLCM and LBP. Initially the features from the HOG, SWT and LBP features are extracted. In addition, the features from the SWT is given as the input to the GLCM to improve the recognition performance of the biometric systems. The description about the feature extraction is explained below,

3.2.1. HOG

HOG technique that has been used in its mature form in Scale Invariant Features Transformation and it has been widely exploited in human detection.HOG descriptor is based on the accumulation of gradient directions over the pixel of a small spatial region referred as "cell" and in the subsequent construction of a 1D histogram whose concatenation supplies the features vector to be considered for further purposes. Let L be an intensity (grayscale) function describing the image to be analyzed. The image is divided into cells of size $N \times N$ pixels and the orientation $\theta_{x,y}$ of the gradient in each pixel is computed by means of the following rule.

$$\theta_{x,y} = \tan^{-1} \frac{L(x,y+1)-L(x,y-1)}{L(x+1,y)-L(x-1,y)} \quad (2)$$

Successively, the orientations $\theta_i^j\, i = 1 \ldots N^2$, i.e. belonging to the same cell j are quantized and accumulated into a M-bins histogram. Finally, all the achieved histograms are ordered and concatenated into a unique HOG histogram that is the final outcome of this algorithmic step, i.e. the features vector to be considered for the subsequent processing.

3.2.2. STATIONARY WAVELET TRANSFORM

The Stationary Wavelet Transform (SWT) is a recent type of wavelet transform family that is similar to the Discrete Wavelet Transform (DWT). It is designed to overcome the lack of translation-invariance in the Discrete Wavelet Transform by suppressing the process of downsampling and up-sampling in the DWT. This means that SWT is translation-invariant and is designed by upsampling only the filter coefficients by a factor of $2(j-1)$ in the j^{th} level of the algorithm. SWT follows an inherently redundant scheme as each of its output levels contains the same number of samples as the input. For a decomposition of N levels there is a redundancy of N in the wavelet coefficients. The decomposition values of SWT are given in the equations (3-6).

$$A_{j,k1,k2} = \sum_{n1}\sum_{n2} h_0^{\uparrow 2^j}(n1-2k_1)h_0^{\uparrow 2^j}(n2-2k_2)A_{j-1,n1,n2} \quad \ldots\ldots(3)$$

$$D^1_{j,k1,k2} = \sum_{n1}\sum_{n2} h_0^{\uparrow 2^j}(n1-2k_1)g_0^{\uparrow 2^j}(n2-2k_2)A_{j-1,n1,n2} \quad \ldots\ldots(4)$$

$$D^2_{j,k1,k2} = \sum_{n1}\sum_{n2} g_0^{\uparrow 2^j}(n1-2k_1)h_0^{\uparrow 2^j}(n2-2k_2)A_{j-1,n1,n2} \quad \ldots\ldots(5)$$

$$D^3_{j,k1,k2} = \sum_{n1}\sum_{n2} g_0^{\uparrow 2^j}(n1-2k_1)g_0^{\uparrow 2^j}(n2-2k_2)A_{j-1,n1,n2} \quad \ldots\ldots(6)$$

Where, $A_{j,k1,k2}$, $D^1_{j,k1,k2}$, $D^2_{j,k1,k2}$ and $D^3_{j,k1,k2}$ are the low frequency components (LL), the horizontal high-frequency component (LH), vertical high-frequency component (HL) and diagonal components (HH) of the stationary wavelet transform, respectively. $h_0^{\uparrow 2^j}$ and $g_0^{\uparrow 2^j}$ are used to denote that 2^{j-1} zeros are inserted between the two points h_0 and g_0.

3.2.2.1. GRAY LEVEL CO-OCCURRENCE MATRIX

The features from the SWT is given as the input to the GLCM. GLCM is used for extracting the second order statistical texture features and it is introduced by Haralick. GLCM transforms the image into a matrix with respect to the pixels of an original image. The calculation of mutual occurrence of pixel pairs is required and it is calculated for a specific distance oriented at a particular direction. Then the statistical features are extracted for further process. The elements of GLCM is divided into four orientations. There are 11 types of features are extracted from the GLCM of pre-processed face image. The extracted features are Auto correlation, Contrast, Correlation, energy, Entropy, Homogeneity, sum average, sum entropy, sum variance, difference variance and difference entropy.

3.2.2.2. LOCAL BINARY PATTERN

Local Binary Pattern (LBP) is used for extracting the features from the pre-processed images and generally it is an operator for texture description that based on the signs of differences between neighbor pixels and central pixels. For each pixel value in the image, a binary code is obtained by thresholding its neighborhood with the value of the center pixel. This binary code can be considered as a binary pattern. The neighbor pixel becomes 1 if the pixel value is greater than or equal to threshold value, and it becomes 0 if the pixel value is less than threshold. Next, the histogram will be constructed to determine the frequency values of binary patterns. Each pattern represents possibility of binary pattern found in the image. The number of histogram bins depends on the number of involved pixels in LBP calculation. The basic version of LBP operator uses the center pixel value as threshold to the 3×3 neighbor pixels. Threshold operation will create a binary pattern representing texture characteristic. The equation basic of LBP can be given as follows in equation (7).

$$LBP(x_c, y_c) = \sum_{n=0}^{7} 2^n g(I_n - I(x_c - y_c)) \qquad (7)$$

here, $LBP(x_c, y_c)$ is the LBP value of center pixel. I_n and $I(x_c - y_c)$ are the values of neighbour pixel and centre pixel respectively. Index n is the index of neighbour pixels. The function $g(x)$ will be zero if $x < 0$ and $g(x) = 1$ if $x \geq 0$.

3.3. FEATURE SELECTION USING KNN BASED GENETIC ALGORITHM

The feature selection selects the best features from the hybrid feature extraction. The classification involves consideration of database before transferring the data to a classifier. It is recommended to consider only an important feature for selection. Hence, it is useful for choosing the significant and relevant features in this finger vein pattern. Furthermore, the feature selection is used during the classification to find the important feature that decrease the workload of the classifier and enhances the classification accuracy. In this research work, KNN based GA significantly reduces the redundancy with-in the input voxels and also determines the maximum relevance between output and input voxels. In initial stage, generate the initial population, which is set as the subset for input voxels. Next, the fitness function is computed for input voxel subsets utilizing the KNN distance algorithm that increases the mutual-information between the voxels. Finally, crossover and mutation operators are used to find the most active voxels by decreasing the redundancy based on the fitness function. The GA selects the subset of features as the chromosomes and every chromosome is sent to the SVM for computing fitness value. The SVM classifier employs each chromosome as a mask for capturing the features. The SVM classifier defines a fitness value of each and every chromosome and GA utilizes these fitness values for the chromosome computation process. At the final stage, the GA finds an optimal subset of the feature.

3.4. SECURITY ENHANCEMENT USING DUAL RSA

Dual RSA have been introduced in this proposed methodology for improving the confidentiality of the biometric system. The extracted features from the HOG, GLCM and LBP are encrypted and it is trained in the ECOC-SVM. These encrypted features are decrypted during the testing process. In dual RSA two instances of RSA will share the same public and private key exponents. So it will reduce the memory requirements required for storing both keys because both key exponents are same. Twin RSA is also used to reduce storage requirements.

3.4.1. KEY GENERATION ALGORITHM

Input: Generate or choose large random prime numbers.
Output: Public Key $(e, n1, n2)$ and private key $(d1, d2, p1, q1, p2, q2)$.

1. Four different prime numbers such as $p1, p2, q1$ and $q2$ is generated.
2. Compute the modulus $n1 = p1 \times q1$ and $n2 = p2 \times q2$
3. Compute the $\varphi 1(n1) = (p1 - 1) \times (q1 - 1)$ and $\varphi 2(n2) = (p2 - 1) \times (q2 - 1)$
4. Choose for public exponent an integer e such that $\varphi 1(n1) < e < \varphi 2(n2)$ and $gcd(e, \varphi 1(n1), \varphi 2(n2)) = 1$.
5. Compute the private exponent $d = e^{-1} mod \varphi(n)$ (employing the extended euclidean algorithm).
6. Public key=$(e, n1, n2)$.
7. Private key$(d1, d2, p1, q1, p2, q2)$.

3.4.2. DUAL RSA ENCRYPTION ALGORITHM

Input: Here the plain text which is given to the RSA encryption is the features from the finger vein pattern.

Output: The encrypted cipher-text.

1. Obtain authentic public key(n, e).
2. Calculate $Y = F_v^{\ e} mod n. (i.e., n = gcd(n1, n2))$
3. Deliver the cipher text c to A.

This RSA encryption gives three different cipher texts such as face & iris, iris & palm, face & palm and these cipher texts are stored in three different databases.

3.4.3. DUAL RSA DECRYPTION ALGORITHM

Input: The receiver's private key $(d1\ or\ d2)$ and the received encrypted cipher text
Output: The original plain text.
Use the private key $d1\ or\ d2$ to recover

$$F_v = Y^{d1} mod n \text{ or } F_v = Y^{d2} mod n$$

3.5. CLASSIFICATION USING ECOC-SVM

The bits of error occurred in the processing of image is corrected by ECOC and also this ECOC resolves multi class learning problems. The main steps behind the learning classification of ECOC is stated as follows:

1. The n bit code which has the minimum hamming distance d is created.
   Where $n \geq [log_2 K] + d$.
2. The unique code word is allocated to training samples of each class for specifying the class.
   The code word for training sample Y is represented as $C(k)$ for class k. Here Y is the encrypted vector.

   The following Eq. (8) describes the training set of the ECOC-SVM.

$$S_Y = \{(Y, C(k)), k = 1, \ldots, K\} \quad (8)$$

   The training set has n binary functions, $f_i(Y)\ (i = 1, \ldots, n)$ with the f_i corresponding to the i-th bit of $C(k)$.
3. The n binary functions are learned from the training set (S_Y) with the help of learning algorithm.

After finishing training stage, a new input sample Y_{new} is classified by n learned functions such as $\hat{f}_i(Y), (1 = 1, \ldots., n)$. This classification is happened by achieving the n binary output values that is given in the following Eq. (9).

$$\hat{y}_i = u[\hat{f}_i(Y_{new})]\ (i = 1, .. n) \quad (9)$$

Where $u(Y) = \begin{cases} 1\ if\ Y \geq 0 \\ 0\ Otherwise \end{cases}$

Here, the n binary outputs are generated as a one code word and this code word send via error correcting algorithm. Finally, the classification result is achieved by decoding the corrected code word. The theory of error control coding says, the ECOC classification corrects up to $[(d-1)/2]$ errors happened in $\hat{y}_i\ (i = 1, .. n)$. At last, the trained values from the fusion are saved and further it is utilized in the testing process. The classification among the query image and to the trained database is performed by this ECOC-SVM.

4. RESULTS and DISCUSSION

The proposed methodology is analyzed with the help of MATLAB 2017b and the work was done on I3 system with 2GB RAM. This biometric system is developed based on finger vein pattern. The security over the Unimodal enhanced by using Dual RSA. The performance of the proposed methodology is analyzed in terms of accuracy, precision, recall, false acceptance rate and false rejection rate.

4.1. DATABASE DESCRIPTION

In order to prove the effectiveness of the proposed methodology,the database used here is named as Homologous Multi-modal traits Database (SDUMLA-HMT Database) provided by shandong university. SDUMLA-HMT Database contains face, finger print, iris, gait vein and other biometrics. In this proposed methodology only the finger vein database is used in the experiments. The sample images from the SDUMLA-HMT

4.2. PERFORMANCE ANALYSIS

In this proposed methodology, 10 users are considered to develop the secure unimodal biometric systems with finger vein pattern image. Here totally 180 images (18 images from each person) are taken from the SDUMLA-HMT Database for creating the database. From the 180 images, the features are extracted by using the hybrid feature extraction technique which is clearly explained in the above section. From the group of features, the optimized features are selected by KNN based genetic algorithm. The extracted features are encrypted using dual RSA cryptography technique and it is trained in the ECOC-SVM. Finally, the trained features from the SVM is stored as the database. In testing section 30 images that is 3 images from each person is taken for testing the recognition rate of proposed methodology. The feature extraction, feature selection of the testing side is similar to the training section. The trained features are decrypted and then this is evaluated with the testing image.

The performance is analyzed in two different ways one is when the system doesn't affect by any of the attacks and another one is when the system is affected by any of the spoofing attacks. From the finger vein classification, four different parameters True Positive (TP), True Negative (TN), False Positive (FP) and False Negative (FN) are calculated. This TP, TN, FP and FN are used for calculating the performance. The performance parameters analyzed in this proposed methodology method are described as follows:

a. Accuracy

Accuracy is defined as the computation of closeness between the input image and the trained database. The accuracy is expressed in the Eq. (10).

$$Accuracy = \frac{TP+TN}{TP+FP+TN+FN} \qquad (10)$$

b. Sensitivity

Sensitivity is described as the true positive rate or the recall rate for measuring the proportion of actual positives. The sensitivity is expressed in Eq. (11).

$$\text{Sensitivity} = \frac{TP}{TP+FN} \qquad (11)$$

c. Specificity

Specificity is defined as the percentage of people who are perfectly discovered as an authorized person. It gives proportion of negatives and the specificity is shown in the Eq. (12).

$$\text{Specificity} = \frac{TN}{FP+TN} \qquad (12)$$

d. False acceptance rate (FAR)

The FAR is the measure of the likelihood that the biometric security system will incorrectly accept an access attempt by an unauthorized user.

e. False Rejection rate (FRR)

The FRR is the measure of the likelihood that the biometric security system will incorrectly reject an access attempt by an unauthorized user.

Table 1. Performance analysis of proposed methodology with attacks

Performances	**SNR=1**	**SNR=5**	**SNR=9**	**SNR=13**	**SNR=17**	**SNR=21**	**SNR=25**	**SNR=29**
accuracy	0.566667	0.800000	0.733333	0.900000	0.900000	0.933333	0.933333	0.966667
sensitivity	0.666667	0	0.333333	0.333333	0.333333	1.000000	1.000000	1.000000
specificity	0.555556	0.888889	0.777778	0.962963	0.962963	0.925926	0.925926	0.962963
precision	0.14	0	0.14	0.50	0.50	0.60	0.60	0.7

	2857		2857	0000	0000	0000	0000	50000
recall	0.666667	0	0.333333	0.333333	0.333333	1.0000000	1.0000000	1.0000000
f_measure	0.235294	0	0.2000000	0.4000000	0.4000000	0.7500000	0.7500000	0.857143
gmean	0.608581	0	0.509175	0.566558	0.566558	0.962250	0.962250	0.981307
FAR	16	25	22	27	27	26	26	27
FRR	7	Inf	8	3	3	0.666667	0.666667	0.333333
MSE	0.751632	0.282992	0.122428	0.056384	0.020084	0.008097	0.003293	0.001271
PSNR	1.239945	5.482253	9.121180	12.488427	16.971510	20.916840	24.824352	28.958797

Table 1 shows the performance of the proposed methodology with attack. The proposed methodology shows the proposed methodology gives 96.67% of accuracy during the recognition process. Meanwhile the PSNR value of the proposed methodology increases while increasing the SNR value. Similarly, the mean square error also decreased by increasing the SNR. From the increment in PSNR, conclude that the proposed method gives effective performance when the system affected in any spoofing attacks. Moreover, the confidentiality of the proposed methodology is increased by the Dual RSA cryptography technique.

4.3. COMPARATIVE ANALYSIS

The effectiveness of the proposed methodology is known by comparing the proposed methodology with two existing methods such as ANOVA [20] and PB-SIFT [21]. The ANOVA were analyzed by four classifiers such as ANN, SVM, KNN and DNN. The comparison of the proposed methodology with ANOVA [20] and PB-SIFT [21] is given in the following :

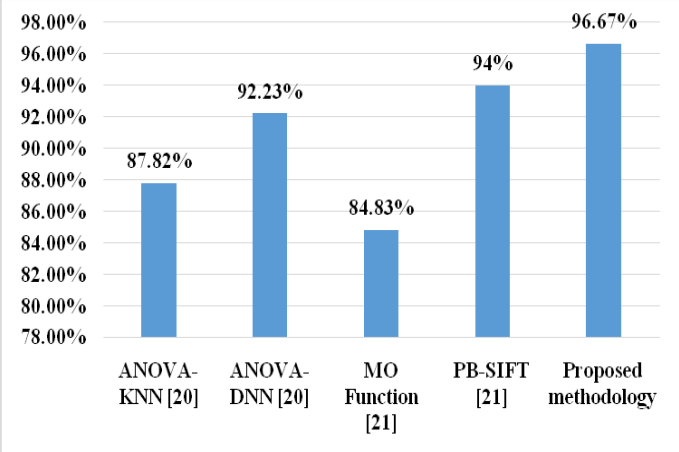

Figure 3. Comparison of accuracy for different methods

The performance of the proposed methodology is high when compared to other methods named as ANOVA [20] and PB-SIFT [21]. Because, here hybrid feature extraction is used in this proposed methodology as well as selective features are selected by using KNN based genetic algorithm.

5. CONCLUSION

In this paper, the finger vein pattern is used as a biometric trait because finger-vein pattern remains unchanged or constant throughout human lifeand finger-vein is an internal feature hidden in human body, making it secure compared to other biometric patterns. There are four

different feature extraction methods are used in this proposed methodology such as HOG, SWT, GLCM and LBP. The recognition rate of the proposed methodology is increased by two ways. One is the features from the SWT is given as the input to the GLCM and another one is taking the selective feature from the set of features. The feature selection is performed by using the KNN based genetic algorithm. The confidentiality of the biometric system is improved by Dual RSA which is used to perform against the spoofing attacks. The accuracy of the proposed methodology is 96.67%, it is high when compared to the existing methods such as ANOVA and PB-SIFT.

REFERENCES

[1] Kim, D.J., Shin, J.H. and Hong, K.S., 2010. Teeth recognition based on multiple attempts in mobile device. Journal of Network and Computer Applications, 33(3), pp.283-292.

[2] Aly I. Desoky, Hesham A. Ali, Nahla B. Abdel-Hamid, "Enhancing iris recognition system performance using templates fusion",Ain Shams Engineering Journal (2012) 3, 133–140.

[3] Jain, Y. and Juneja, M., 2017. A comparative analysis of iris and palm print based unimodal and multimodal biometric systems. In Innovations in computer science and engineering (pp. 297-306). Springer, Singapore.

[4] Shaikh, S.A. and Rabaiotti, J.R., 2010. Characteristic trade-offs in designing large-scale biometric-based identity management systems. Journal of Network and Computer Applications, 33(3), pp.342-351.

[5] Hsia, C.H., Guo, J.M. and Wu, C.S., 2017. Finger-vein recognition based on parametric-oriented corrections. Multimedia Tools and Applications, 76(23), pp.25179-25196.

[6] Rattani, A., Marcialis, G.L. and Roli, F., 2013. Biometric system adaptation by self-update and graph-based techniques. Journal of Visual Languages & Computing, 24(1), pp.1-9.

[7] Nair, S.A.H. and Aruna, P., 2015. Comparison of DCT, SVD and BFOA based multimodal biometric watermarking systems. Alexandria Engineering Journal, 54(4), pp.1161-1174.

[8] Meraoumia, A., Chitroub, S. and Bouridane, A., 2014. Biometric recognition systems using multispectral imaging. In Bio-inspiring Cyber Security and Cloud Services: Trends and Innovations (pp. 321-347). Springer, Berlin, Heidelberg.

[9] V A Bharadi and H B Kekre, "Off-Line Signature Recognition Systems", International Journal of Computer Applications (0975 - 8887) Volume 1 – No. 27.

[10] Wojtowicz, W. and Ogiela, M.R., 2016. Digital images authentication scheme based on bimodal biometric watermarking in an independent domain. Journal of Visual Communication and Image Representation, 38, pp.1-10.

[11] Kim, Y., Yoo, J.H. and Choi, K., 2011. A motion and similarity-based fake detection method for biometric face recognition systems. IEEE Transactions on Consumer Electronics, 57(2).

[12] De Marsico, M., Nappi, M., Riccio, D. and Tortora, G., 2009. A multiexpert collaborative biometric system for people identification. Journal of Visual Languages & Computing, 20(2), pp.91-100.

[13] Matveev, I., Novik, V. and Litvinchev, I., 2018. Influence of degrading factors on the optimal spatial and spectral features of biometric templates. Journal of Computational Science, 25, pp.419-424.

[14] Liu, Z., Yin, Y., Wang, H., Song, S. and Li, Q., 2010. Finger vein recognition with manifold learning. Journal of Network and Computer Applications, 33(3), pp.275-282.

[15] Li, S., Zhang, H., Jia, G. and Yang, J., 2018, August. Finger Vein Recognition Based on Weighted Graph Structural Feature Encoding. In Chinese Conference on Biometric Recognition (pp. 29-37). Springer, Cham.

[16] Ong, T.S., William, A., Connie, T. and Goh, M.K.O., 2018. Robust hybrid descriptors for multi-instance finger vein recognition. Multimedia Tools and Applications, pp.1-29.

[17] Gumaei, A., Sammouda, R., Al-Salman, A.M.S. and Alsanad, A., 2019. Anti-spoofing cloud-based multi-spectral biometric identification system for enterprise security and privacy-preservation. Journal of Parallel and Distributed Computing, 124, pp.27-40.

[18] Tahmasebi, A. and Pourghassem, H., 2017. Robust Intra-Class Distance-Based Approach for Multimodal Biometric Game Theory-Based Rank-Level Fusion of Ear, Palmprint and Signature. Iranian Journal of Science and Technology, Transactions of Electrical Engineering, 41(1), pp.51-64.

[19] Xie, S.J., Yoon, S., Yang, J., Lu, Y., Park, D.S. and Zhou, B., 2014. Feature component-based extreme learning machines for finger vein recognition. Cognitive Computation, 6(3), pp.446-461.

[20] Semwal, V.B., Singha, J., Sharma, P.K., Chauhan, A. and Behera, B., 2017. An optimized feature selection technique based on incremental feature analysis for bio-metric gait data classification. Multimedia tools and applications, 76(22), pp.24457-24475.

[21] Meng, X., Xi, X., Yang, G. and Yin, Y., 2018. Finger vein recognition based on deformation information. Science China Information Sciences, 61(5), p.052103.