

International Journal of Research in Management, Science and Technology

Issue - 12, Vol-06, pp. 85-97, Jul-Dec 2016 CLEAR International Journal of Research in Management, Science and Technology

RESEARCH ARTICLE

FUSION OF KNUCKLE PRINT AND IRIS FOR MULTIMODAL BIOMETRIC RECOGNITION AND CRYPTOGRAPHIC KEY GENERATION

P. Sivakumar¹, Dr. S. Senthamarai Kannan², Dr. S. Appavu Balamurugan³
 ¹Associate Professor, OCET, Theni, ²Professor, MIET, Madurai, ³ Professors, KLNIT, Madurai Shiva_2476@yahoo.com, stanfordssk@gmail.com, <u>app_s@yahoo.com</u>

ABSTRACT

Article History:

Received 22th Nov 2016 Received in revised form 28th Nov 2016 Accepted 28.11.2016 Published on 30.12.2016

Keywords—Multi-Model Biometrics, Cryptanalysis,privacy, Public key Cryptography, security

Corresponding author:

P. Sivakumar¹ Email: Shiva_2476@yahoo.com,

It is very difficult to remember long cryptographic keys by a human being since they are formed by the combinations of alphanumeric with special characters. Hence the researcher have been trying to find some alternate way for authentication in the client server application that is from human being biometric traits instead of remembering longer complex password or passphrase. It is an attempt to generate cryptographic keys from user's biometric features which are tough to cryptanalysis and unpredictable for a hacker to crack any information from the compromised biometric. This work proposes an efficient approach based on Multi-Model Biometric system (Fusion of Knuckle and Iris) for the Client Server Authentication processes. Features are selected from both Knuckle and Iris, the extracted features are encrypted by RSA algorithm and stored as a template in the database. The query input (both Knuckle and Iris) is processed by the same way and matched with the template stored in the data base. The experimental results have proved that Multi-Model Biometric system is having the capability of providing better user



International Journal of Research in Management, Science and Technology

1. Introduction

Biometrics is the science and technology of measuring and analyzing biological data of human body, extracting a feature set from the acquired data, and comparing this set against to the template set in the database [1]. Biometricbased techniques have emerged as the most promising option for recognizing individuals in recent years. Basically we identify the people using passwords, PINs, smart cards, tokens, keys etc. but these are sometimes misplaced, forgotten, purloined or duplicate and hard to remember. However an individual's biological traits cannot be misplaced, forgotten, stolen or forged. Biometric-based technologies include identification based on physiological characteristics (such as face, fingerprints, finger geometry, hand geometry, hand veins, palm, iris, retina, ear and voice) and behavioral traits (such as gait, signature and keystroke dynamics) [2].Human physiological and/or behavioral characteristic can be used as a biometric trait when it satisfies the requirements like ubiquity, peculiarity, stability and collectability. In practice, no single biometric can satisfy all the desirable characteristics mentioned above for it to be used for person authentication. This is due to the problems associated with noisy data, intra-class variation, non-universality, spoof attacks and high error rates [4]. To overcome this limitation, multiple biometric features can be used for person authentication. This resulted in the development of multimodal biometric person authentication system [4]. Thus biometric system can be classified as uni-modal system and multimodal system based on whether single or multiple biometric features are used for person authentication. Biometric security system

becomes a powerful tool compared to electronics based security systems [3].

Multimodal authentication biometric techniques attract much attention of many researches recently as the fusion between many different modalities can increase the recognition rate. The fusion can be achieved in different levels such as sensor, feature, or classification level. The literature reported that the multimodal biometric methods achieve better recognition rates than unimodal biometric methods. From the uni-modal biometrics data, two traits of iris [5] and finger knuckle [6] are recently best authentication biometrics. The finger knuckle biometrics is emerging as the full proof method of automated personal identification. Similar to fingerprint, these dermal patterns are formed at birth and they will not change throughout the life of a person. These line features are reliable and they can serve as unique personal identifier. Moreover, these line textures are clearly visible on the hand's upper surface and they can be captured using relatively inexpensive low resolution device [7]. Moreover, iris recognition system (IRS) is most efficient and reliable system [8] for authentication check. Generally, Feature selection strategies often are applied to explore the effect of irrelevant the performance of classifier features on systems [9-11]. In this phase, an optimal subset of features which are necessary and sufficient for solving a problem is selected. Feature selection improves the accuracy of algorithms by reducing the dimensionality and removing irrelevant features [12] [13]. Feature level fusion, signals coming the iris and finger knuckle biometric traits is first processed and feature vectors are extracted separately from the each biometric trait [14].



The multimodal-based authentication can help the system in increasing the security and efficiency in contrast to uni-modal biometric authentication, and it would be very difficult for an adversary to spoof the system because of two distinct biometrics traits [26]. Recently, multimodal biometrics fusion techniques have attracted much attention as the supplementary information between different modalities could recognition improve the performance [27].Information from different biometrics traits can be integrated at the feature level (integrating the features of different biometrics), score level (combining the genuine and imposter scores), or decision level (combining the decisions). Although feature sets are the rich source of information, features from these modalities may not be compatible. Moreover large dimensionality of a feature space may lead to irrelevant and the redundant information [15]. In addition, the scores are combined from two face recognition experts and one speaker recognition expert using three classifiers: k-NN classifier using vector quantization, decision-tree based classifier and a classifier based on a logistic regression model [16]. Fuzzy k-means and fuzzy vector quantization, along with a median radial basis function neural network classifier is implemented for the fusion of scores obtained from biometric systems based on visual (facial) and acoustic (vocal) features[17]. Score level fusion of iris and fingerprint biometrics is carried out via Support Vector Machine (SVM) [18].Score level fusion for iris recognition is achieved by using HD (Hamming distance) produced by a Gabor filter [19]. Cryptographic key generation is a method recognizes the human very secure. One effective solution with added security is the incorporation of multimodal biometrics into cryptographic key

generation; so as to achieve incredible security against cryptographic attacks.

2. Review of related works:

In the literature survey, several methods have been proposed for the biometric recognition in human authentication. Among the most recently published works are those presented as follows:

MadasuHanmandlu*et* al. [20] have explained the Score level fusion of multimodal biometrics using triangular norms. A multimodal biometric system that alleviates the limitations of the uni-modal biometric systems by fusing the information from the respective biometric sources was developed. A general approach was explained for the fusion at score level by combining the scores from multiple biometrics using triangular norms (t-norms) due to Hamacher, Yager, Frank, Schweizer and Sklar, and Einstein product. This study aims at tapping the potential of t-norms for multimodal biometrics. The approach renders good performance as it was quite verv computationally fast and outperforms the score level fusion using the combination approach (min, mean, and sum) and classification approaches like SVM, logistic linear regression, MLP, etc. The experimental evaluation on three databases confirms the effectiveness of score level fusion using t-norms.

Moreover, Swathi*et al.* [21] have explained the DWT-based Feature Extraction and Radon Transform Based Contrast Enhancement for Improved Iris Recognition.In this paper, a method for recognition of iris patterns was explained by using a combination of preprocessing using Radon transform and Top hat filtering, feature extraction using Discrete Wavelet Transform (DWT) and Discrete Cosine



International Journal of Research in Management, Science and Technology

Transform (DCT), and feature selection using Binary Particle Swarm Optimization. Individual stages were examined and an attempt was made to improve each stage. Radon transform was used for detecting lines present in the iris textures and Top hat filtering was used for image enhancement. A combination of DWT and DCT was used to extract the salient iris features. A BPSO-based feature selection algorithm was used to search the feature vector space for the optimal feature subset.

In, Lan Linet al. [22] get planned a geometric face model of human skull structure based on the Frankfurt horizontal plane of a human skull. As outlined by their particular face type, the compensating angle has been determined in the SCA for a face image used exactly the same lighting method. Using the compensating angle, the illumination compensation for a face image has been performed by simply an additive component procedure. Their own experimental outcomes confirmed their particular technique for the Yale B face database. In contrast to Choi's techniques, their technique has been increased the particular images along with significant lighting angle, and it has been better made to light change in both horizontal and vertical directions.

Similarly,Patricia Melin*et.al.*[23] have suggested genetic optimization of modular neural networks with fuzzy response integration for human recognition. They explained new method to genetic optimization of modular neural networks with fuzzy response integration. Here, they explained the technique was connected to the instance of human recognition based on three biometric measures, specifically iris, ear, and voice. The experimental results demonstrated that optimal modular neural networks could be

designed with the utilization of genetic algorithms and as a consequence the recognition rates of such systems could be enhanced fundamentally. On account of optimization of the fuzzy framework for response integration, the genetic algorithm not just changes the quantity of membership functions and principles, additionally permitted the variety on the kind of logic (type-1 or type-2) and the changed in the derivation model. An alternate fascinating finding of their work was that when human recognition was performed under noisy conditions, the response integrators of the modular networks built by the genetic algorithm were discovered to be optimal when utilizing type-2 fuzzy logic. This could had been anticipated as there had been evidence from past works that type-2 fuzzy logic was more qualified to model larger amounts of instability.

Additionally, Shoichiro Aoyamaet al. [24] have explained the finger-knuckle-print recognition algorithm using Band-Limited Phase-Only Correlation (BLPOC)-based local block matching. The phase information obtained from 2D Discrete Fourier Transform (DFT) of images important information of contains image representation. The phase-based image matching, especially BLPOC-based image matching was successfully applied to image recognition tasks for biometric recognition applications. То calculate the matching score, the algorithm corrects the global and local deformation between FKP images using phase-based correspondence matching and the BLPOC-based local block matching, respectively. Experimental evaluation using the PolyU FKP database demonstrates the efficient recognition performance of the algorithm compared with the state-of-the-art conventional algorithms.



International Journal of Research in Management, Science and Technology

Moreover, JialiangPenget al. [25] have Multimodal biometric explained the authentication based on score level fusion of finger biometrics. Here, finger multimodal biometric authentication that combines finger vein, fingerprint, finger shape and finger knuckle print features of a single human finger. The multimodal biometrics provides score-level fusion approach based on triangular norm with four finger biometric traits, instead of two or three ones combined in the previous approaches. The experimental evaluations and analysis were conducted on a merged multimodal biometrics database. The results were show that the scorelevel fusion approach using triangular norm obtains a larger distance between genuine and imposter score distribution as well as achieves lower error rates. Moreover, the comparison results suggest that the score level fusion of finger biometrics using triangular norm outperforms the state-of-the-art approaches.

3. Problem Definition and Proposed Methodology:

Most real-life biometric systems are still uni-modal. Uni-modal biometric systems perform person recognition based on a single source of biometric information. Such systems are often affected by some problems such as noisy sensor data, non-universality and spoof attacks. Multibiometrics overcomes these problems. Multibiometric systems represent the fusion of two or more uni-modal biometric systems. Such systems are expected to be more reliable due to the presence of multiple independent pieces of evidence. Keeping all these requirements in mind, biometric traits like fingerprints, hand veins, handwritten signatures, retinal patterns, ear patterns, electrocardiogram etc. are used extensively in areas which require security access. Among various kinds of biometric identifiers, hand-based biometrics has been attracting considerable attention over recent years due to its ease in accession. Biometric traits like fingerprint, palm print, hand geometry and hand vein and iris have been proposed and well investigated in the literature.

Additionally, human users have a tough time remembering long cryptographic keys. Hence, researchers, for so long, have been examining ways to utilize biometric features of the user instead of a memorable password or passphrase, in an effort to generate strong and repeatable cryptographic keys. The main objective of this research is to incorporate the volatility of the user's biometric features into the generated key to biometric identification and encryption. The goal of my research will be done in two phases in multi-model biometrics.

PHASE-1:

In this phase, the two set features will be extracted from iris and finger images. At first, the finger image will be preprocessed to get the finger ROI (Region of interest), and knuckle print features of index, middle, ring and little fingers will be extracted from the finger ROI. On other hand, localization process will be applied on the iris images; some useful features will be extracted. Subsequently, the extracted features will be fused together at the feature level to construct the multi-biometric template. After that, a 256-bit secure cryptographic key will be generated from the multi-biometric template. Finally, based on the 256-bit secure cryptographic key, the applications related to recognition and encryption will be done.



International Journal of Research in Management, Science and Technology

PHASE-2:

In this phase, some additional features will be selected based on iris and knuckle print of image presented in the database. The additional features provided based on iris and knuckle print image will provide the significant improvement as compared with existing algorithm. The implementation will be done in MATLAB and the performance of the algorithms will be analyzed using false alarm rate (FAR), False rejection rate (FRR) and accuracy.

4. Implementation Results:

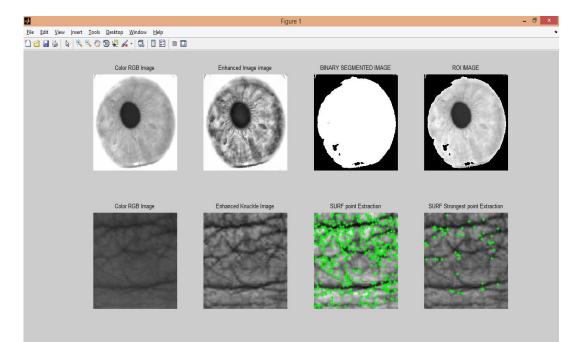
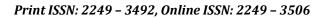


Figure 1: Image processing stepsat Client Side

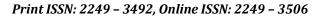




A					MA	TLAB R2013a						-	_
HOME PLOTS A	PPS									4 1 1 2	₫ ₿	③ Search Documentation	٩
New New Open 2 Compare Data	ort Save	New Variable	~		Simulink Library	Layout Cenvironmen	ath Help	Community	upport				
🛚 🔶 🔁 🔀 🐌 🕨 D: 🕨 Projects2017	7 + DSP pro	jects + ATDSP-phd siva	kumar 🕨 pape	r2 + code +									•
Current Folder	۲	Workspace								Ŧ	Com	mand History	
🗋 Name 🔺		Name 🔺	Value	M	lin Max							<pre>% M = feature;</pre>	
l 퉬 data		Command Windo	w							G		x=length(M);	
🗼 data1 🖄 colorMoments.m		New to MATLAB?	Natch this <u>Vide</u>	o, see <u>Example</u>	es, or read Ge	ting Started.				;	()	c=M; *%%Encryption	
🚈 crypt.m		Query IRIS a	nd Knuckle	print Fea	ture					,		for j= 1:x	
會 getmapping.m 會 intialize.m		feturetest =		-								cipher(j) = crypt(c(j), end	Pk,e);
kmeans.m kmeans_clustering.m knn.m		1.0e+07 *									-	out=[out cipher(:)]; end	
libp.m lowpassfilter.m		Columns 1 :	-									<pre>out=[]; for i=1:size(feturetra</pre>	
main_code.asv		0.1392 Columns 10	0.3081	0.5432	1.0302	0.1363	0.3015	0.5221	0.9895	0.1449		<pre>p = 47;%input('\nEnter q = 37;%input('\nEnter</pre>	the t
Multisvm.m server_part.asv server_part.m		0.3158	0.5269	0.9792	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000		<pre>[Pk, Phi, d, e] = intiali M=feturetrain(:,i); % M = feature;</pre>	ze(p,
test.mat thresh.m		Columns 19	through 21	,							-	<pre>x=length(M); c=M;</pre>	
Trained.mat Trained1.mat training.asy		0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	-	<pre>%%Encryption for j= 1:x</pre>	
 Itraining.m Itraining1.m 		Columns 28	through 30	5								<pre>cipher(j) = crypt(c(j), end</pre>	Pk,e);
		0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000		<pre>out=[out cipher(:)]; end</pre>	
		Columns 37	through 40)								main code	
etails	^	fx										-	>
- 2 🚔 🔮													2:02 9/28/

Figure 2: Feature of query input.

λ					MA	TLAB R2013a					- 0	×
HOME PLOTS	APPS									1969	定 📴 🕐 Search Documentation	۶
ew New Open 🔁 Compare	Import Save Data Workspac	<u>D</u>	<u> </u>	nd Time Commands 👻	Library	O Prefe	ath Hel;	Request Su				
FILE		variable ects + ATDSP-phd sive		CODE	SIMULINK	ENVIRONMEN	at	RESOURCES				-
urrent Folder	() ()	Workspace	Kullin Pup	ine i coure i						۲	Command History	
Name A	0	-									M = feature;	
data		Name 🔺	Value	M	in Max							
data1		Command Windo								\odot	- c=M:	
ColorMoments.m		New to MATLAB?	Watch this <u>Vide</u>	o, see <u>Example</u>	s, or read Ge	tting Started.				×	**Encryption	
🖄 crypt.m										^	for i= 1:x	
gaborWavelet.m		Intaializing The value of		100							cipher(j) = crypt(c(j), Pk,	.e);
etmapping.m		The public k									end	
kmeans.m		The value of									out=[out cipher(;)];	
kmeans clustering.m		The private key (d) is: 1325									end	
knn.m		Encrypted Feature of Iris Image:									out=[];	
🖄 lbp.m		1.0e+03 *									for i=1:size(feturetrain,	2)
lowpassfilter.m											p = 47;%input('\nEnter th	
main_code.asv		Columns 1	through 9								g = 37;%input('\nEnter th	
Main_code.m M multisvm.m											[Pk, Phi, d, e] = intialize(
server part.asv		0.6814	1.6195	0.7730	0.0190	0.1990	0.8203	1.3930	1.2800	0.9695	M=feturetrain(;,i);	1979
server part.m											M = feature:	
test.mat		Columns 10	through 18	5							x=length(M);	
🖄 thresh.m		0,4150	1.3205	1.3090	0.0770	1,4223	0.0672	1.3241	0.0747	1,2901	c=M;	
Trained.mat		0.1100	1.0200	1.0000	0.0770	1.1220	0.00/2	1.02.11	0.0717	1.2501		
H Trained1.mat		Columns 19	through 21	,							****Encryption	
training.asv training.m											for j= 1:x	
training1.m		1.6897	1.4360	0.0822	1.3814	1.7330	1.3336	0.0477	1.3919	1.2255	cipher(j) = crypt(c(j), Pk,	.e);
											end	
		Columns 28	through 36	5							out=[out cipher(:)];	
											end	
atails	^	0.8292 fx	0.9308	1.2089	1.2323	0.9891	0.5230	0.1844	0.5148	0.5613	main_code	
Talls	^	JX.								~		>
									_			
두 🙆 🚞 🚺		入 [2]									▲ 18 203 (0) and 10 2:03 9/28.	





1			MATLAB R20)13a			- Ø ×
HOME PLOTS	APPS						💼 🔁 🕐 Search Documentation 🛛 🔎
New New Open L Compare I Script FiLE	Morkspace Variable	e 👻 🧭 Clear Commands 👻 CODE	Simulink Layout	Preferences ? Set Path Help Parallel ~ ~	실 Community → Request Support 다 Add-Ons ← RESOURCES		
😓 🔶 🛅 💹 📔 🕨 D: 🕨 Projectsi		vakumar + paper2 + code +					•
Current Folder	Workspace					•	Command History
data data1 colorMoments.m crypt.m	Name ≜ Command Wing		n Max s, or read <u>Getting Starter</u>	L		×	<pre>clc load('test.mat'); %% Test code decrypt p = 47;</pre>
 gaborWavelet.m getmapping.m intialize.m kmeans.m 	Decrypted t test =	est Iris and Knuckle	feature				<pre></pre>
 kmeans_clustering.m knn.m lbp.m lowpassfilter.m main code.asv 	1.0e+03 Columns 1	* through 9					<pre>test(j)= crypt(cipher(j),Pk, end disp('Prime number 1') p = 47</pre>
main_code.asv main_code.m multisvm.m server_part.asv	0.9610 Columns 1	1.4575 0.0530 0 through 18	1.4970 0.21	40 1.0952	1.4950 0.1	670 1.4810	disp('Prime number 2') q = 37 disp('Decrypted test Iris ar
test.mat thresh.m Trained.mat	0.4670 Columns 1	0.2560 0.4360 9 through 27	0.0139 1.27	80 0.8200	0.8630 0.9	858 0.4364	test %% Train code decrypt for i=1:size(out,2) for j= 1:x
H Trained1.mat training.asv training.m training1.m	0.7491	1.5638 1.2112	0.9782 0.25	14 0.0071	0.2050 1.0	588 1.1745	<pre>tr(j) = crypt(out(j,i),Pk,d); end</pre>
taning in	Columns 2 0.9960	8 through 36 1.6640 0.8360	0.0635 1.05	90 0.6773	0.7220 1.1	715 1.7139	<pre>train(:,i)=tr; end cl = knn(test,train',group',</pre>
Details Stopped in debugger	fic Columns 3	7 through 40				~	<pre>L-msgbox(['Classified person i <</pre>
) 📣 🔼 📖						► 18 20 00 and 10 2:07 PM 9/28/2017

Figure 3: Encrypted Feature

Figure 4 : Database key generated by RSA algorithm on server side

A	MATLAB R2013a	- 🗗 🔷
HOME PLOTS APPS		🖪 🖬 🚣 🕼 🕼 🗇 🗭 🔁 🕐 Search Documentation 👂
	New Variable Open Variable Ver Ver Ver Ver Ver Ver Ver Ver Ver	Heb Character Support
FILE	variable CODE SIMULINK ENVIRONMENT projects + ATDSP-phd sivakumar + paper2 + code +	RESOURCES
urrent Folder	Workspace	Command History
Name		output. ROC char errors
	Name A Value Min Max	train feature vectors=train
data data1	Command Window	
ColorMoments.m	New to MATLAB? Watch this Video, see Examples, or read Getting Started.	Crain_Ids-group.;
Colorivioments.m	(1) New to MATLAB: Watch this video, see Examples, or read Getting Started.	<pre>x =length(group);</pre>
evaluate results PhD.m	FRR_01FAR_ver: 0.8889	<pre>^ test_feature_vectors=train;</pre>
aaborWavelet.m	FRR_01FAR_far: 0.8889	test_ids=group;
getmapping.m	VER_001FAR_er: 0.5000	results = nn_classification
🕙 intialize.m	VER_001FAR_tr: 0	output =evaluate_results_Ph
🖄 kmeans.m	VER_001FAR_frr: 0.9444	figure, plot (output.ROC_ver_
lkmeans_clustering.m	VER_001FAR_ver: 0.0556	
🔄 knn.m	VER_001FAR_far: 0	<pre>ylabel('FAR');</pre>
🖄 lbp.m		grid on
lowpassfilter.m	Accuray of Each set	figure.plot(output.ROC miss
main_code.asv		
🚵 main_code.m 🖄 multisym.m	ans =	
nn classification PhD.m		<pre>''ylabel('FRR');</pre>
performance.asy	Columns 1 through 9	-grid on
f performance.m		output.ROC_char_errors
produce CMC PhD.m	87.0000 98.0000 16.6667 22.2222 27.7778 33	.3333 38.8889 44.4444 50.0000 disp('Accuray of Each set')
Produce EPC PhD.m		(output.CMC_rec_rates) *100
M produce_ROC_PhD.m	Columns 10 through 18	
iroc_curve.m		mean (output. ROC char erro
server_part.asv	55.5556 61.1111 66.6667 72.2222 77.7778 83	.3333 88.8889 94.4444 100.0000 disp([num2str(mean(output.
魡 server_part.m		close all
test.mat	Total project Accuray in %	close and
🔄 thresh.m	94.4444 %	
Trained mat	× /* >>	v performance
ained.mat (MAT File)	^ <	
		0.00 BL
- 😂 🚞 🕑 🖪		∽ 😼 📶 🗊 2:32 PM 9/28/201

Figure 5 : Template Generation using by RSA algorithm on server side



International Journal of Research in Management, Science and Technology

4	MATLAB R2013a	_ @ ×
HOME PLOTS APPS		🔄 🚍 🕐 Search Documentation 🛛 🔎 🗖
New New Open C Compare Data Worksput		
	piects > ATDSP-phd sivakumar > paper2 > code >	م -
Current Folder	Workspace	Command History 💿
🗋 Name 🔺	Name A Value Min Max	msgbox(['Classified person i ^
data	Command Window	clc load('test.mat');
colorMoments.m	New to MATLAB? Watch this <u>Video</u> , see <u>Examples</u> , or read <u>Getting Started</u> ×	-%% Test code decrypt
Crypt.m	1.0e+03 * Classified person is:1	p = 47;
getmapping.m intialize.m	Columns 1 through 9	<pre>-q = 37; -[Pk,Phi,d,e] = intialize(p,q)</pre>
 kmeans.m kmeans_clustering.m knn.m 	0.9610 1.4575 0.0530 1.4970 0.2140 1.0952 1.4950 0.1670 1.4810	<pre>-for j= 1:x -test(j)= crypt(cipher(j), Pk,</pre>
👰 lbp.m	Columns 10 through 18	
 lowpassfilter.m main_code.asv main_code.m 	0.4670 0.2560 0.4360 0.0139 1.2780 0.8200 0.8630 0.9858 0.4364	<pre>-p =47 -disp('Prime number 2')</pre>
i multisvm.m	Columns 19 through 27	-q = 37 -disp('Decrypted test Iris an
server_part.m* test.mat thresh.m	0.7491 1.5638 1.2112 0.9782 0.2514 0.0071 0.2050 1.0588 1.1745	test %% Train code decrypt
Trained.mat	Columns 28 through 36	for i=1:size(out,2)
Trained1.mat	0.9960 1.6640 0.8360 0.0635 1.0590 0.6773 0.7220 1.1715 1.7139	<pre>for j= 1:x tr(j) = crypt(out(j,i), Pk,d);</pre>
 training.m training1.m 	Columns 37 through 40	
	1.1563 1.0029 0.8130 1.7185	<pre>end cl = knn(test,train',group', msgbox(['Classified person iv</pre>
Details ^	fx K>>	
Stopped in debugger		
- 2 🚔 🕹 🔺		▲ 10 2:08 PM ▲ 10 2:08 PM 9/28/2017

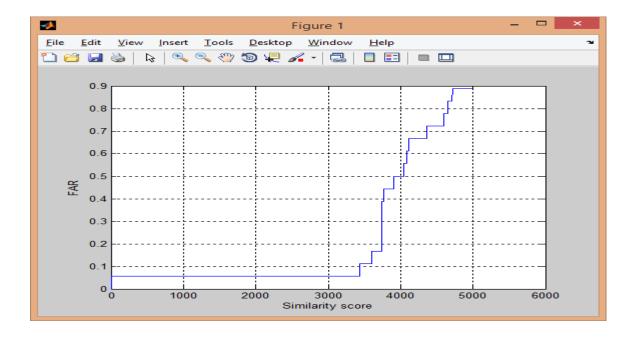
Figure 6: Verification Process

A					MATLAB R2	013a					-	o ×
HOME PLOTS APPS	VARIABLE	VIEW							2 6 %	<u>• • •</u>	🖻 🔁 🕐 Search Documentation	Q
Goven - Rows Column		Transpose										
ew from Print - 1 1		Sort •										
election -	insent Delete ∠	j son ♥										
VARIABLE SELECTION	EDIT											
🔶 🔁 🔀 🎉 🕨 D: 🕨 Projects2017 🕨 D	SP projects + ATDSP-ph	d sivakumar 🕨	paper2 + co	ode 🕨								-
urrent Folder	Workspace									\odot	Command History	
🗋 Name 🔺	Name 🔺	Value		Min I	Лах						clc	
퉬 data										-	<pre>load('test.mat');</pre>	
adata1	Variables -	train								★ (1)	**** Test code decrypt	
🔄 colorMoments.m	🕴 train 🛛 🗶										p = 47;	
crypt.m gaborWavelet.m	🔠 train <40x18	ingle>									q = 37;	
gaborWavelet.m	1	2	3	4	5	6	7	8	9	10	[Pk, Phi, d, e] = intial	ize(p,
intialize.m	1 961	396	540	1024	1024	612	1590	165	- 69		for j= 1:x	
kmeans.m	2 1,4575e+03	375	204	1,2053e+03	1,2053e+03	1030	105	547	1074	8	test(j) = crypt(cipher	(j),P}
kmeans_clustering.m	3 53	1.5275e+03	925	1487	1.2035e+05	288	1660	442	480	8	end	
🕙 knn.m			925		43	288	1672			13	disp('Prime number 1')
🖄 lbp.m		257		43				535	1313		p =47	
lowpassfilter.m	5 214	686.7500	1.0486e+03	962	962	474	1.3189e+03	204	874.2500	3	disp('Prime number 2'	,
main_code.asv	6 1.0952e+03	1626	1721	1245	1245	240	1552	893	1.4129e+03	214.87	q = 37	
🔄 main_code.m 👰 multisym.m	7 1495	651	1.5212e+03	1734	1734	1672	670	292	307	9	disp('Decrypted test	
server part.asv	8 167	155	1091	1399	1399	387	1320	368	696	14 🗸	test	1113 0
server part.m*	<									>		
test.mat	Command W	indow								(7)	%% Train code decrypt	
thresh.m										×	for i=1:size(out,2)	
🛨 Trained.mat	New to MAT						6773 0	.7220 1	.1715		101)- 1	
Trained1.mat	0.998	1.004	0 0.83	0.0	635 1.03	.90 0.	6//3 0	./220 1	.1/15	1.7139 ^	<pre>tr(j) = crypt(out(j,i)</pre>	, Pk, d)
training.asv	Column	37 throug	» 40								end	
training.m	COLUMN	of throug									<pre>train(:,i)=tr;</pre>	
🚵 training1.m	1,156	3 1.002	9 0.81	30 1.7	185						end	
	11100		- 0.01								cl = knn(test,train',	group'
											msgbox(['Classified p	erson
	K>> load	'Trained.m	at')								<pre>load('Trained.mat')</pre>	
ained.mat (MAT File)	^ <i>fx</i> K>>									~		>
opped in debugger												
- 😂 🚞 🕑 🖪	🙏 🛛 🔎 🤎										🔺 🍡 🛃 🕪 📶 📆	

Figure 7 : Performance Analysis



A	MATLAB R2013a	_ Ə ×
HOME PLOTS APPS		😪 🖨 🕐 Search Documentation 🛛 🔎 🛣
New New Open © Compare Data Workspace	New Variable Analyze Code Image: Code	
	variable code sindlink environment resources	م -
Current Folder	Workspace ()	
data	Command Window Command Window	crain_rus-group ,
initialize.m init	ERF_CT: 0.5000 EER_fr: 0.5000 EER_ver: 0.5000 EER_far: 0.5000 FRR_01FAR_er: 0.5000 FRR_01FAR_er: 3.4655+03	<pre>-output =evaluate_results_PhI -figure,plot(output.ROC_ver_r -xlabel('Similarity score'); -ylabel('FAR'); -grid on</pre>
main_code.asv main_code.m Multisvm.m Mnn_classification_PhD.m performance.asv	FRR_01FAR_frr: 0.1111 FRR_01FAR_ver: 0.8889 FRR_01FAR_far: 0.8889 VER_001FAR_er: 0.5000 VER_001FAR_er: 0.5000	<pre>-figure,plot(output.ROC_miss_ -xlabel('Similarity score'); -ylabel('FRR'); -grid on -output.ROC char errors</pre>
performance.m produce_CMC_PhD.m produce_EPC_PhD.m produce_EPC_PhD.m produce_ROC_PhD.m server_part.sv	VER_001FAR_frr: 0.9444 VER_001FAR_ver: 0.0556 VER_001FAR_far: 0 Accuray of Each set	<pre>-disp('Accuracy of Each set'); -(output.CMC_rec_rates)*100 -disp('Total project Accuracy -mean(output. ROC_char_error -disp(Inum2str (mean(output. B)));</pre>
test.mat test.mat test.mat thresh.m Trained.mat (MAT File)	ans = f: Columns 1 through 9 <	<pre>close all</pre>
🗧 🥝 🚞 🕹 🔺		- 🕞 🛃 (II) ad 🕅 2:31 PM 9/28/2017



P. Sivakumar Dr. S. Senthamarai Kannan, Dr. S. Appavu Balamurugan/Management, Science and Technology/2016/94



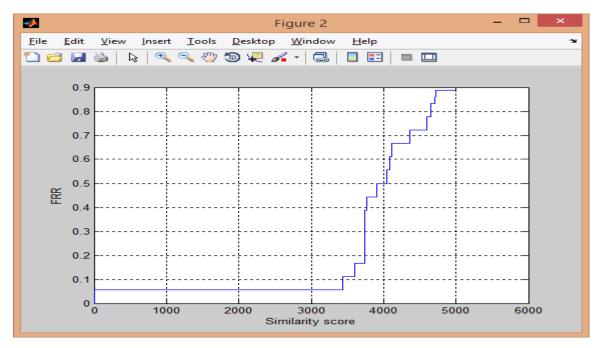


Figure 9: FRR (False Rejection Ratio)

5. CONCLUSION

This work proposed an efficient authentication mechanism from client and server by the use of fusion of biometric traits like Finger Knuckle Print and Iris. This method enhanced the security of the by the fusion of two biometric using Multi- model Biometric System. The proposed approach consists of three modules namely, 1) Feature 2) extraction from Knuckle, Feature extraction from iris 3) Then above two features are fused to generate features and 4) Finally features are encrypted by RSA algorithm and stored as a template in the database.

Any input query requires authentication, the above said steps are repeated and compared with the template in the database. The query input is matching with the template then the corresponding then the given input is authenticated and allowed to access service from the server. For experiment results, data base of finger Knuckle Print images and iris are used. The experimental results have demonstrated the security of the proposed approach to enhance



International Journal of Research in Management, Science and Technology

when compared to the previous methods of Multi- Model Biometrics.

References:

[1] MadhaviGudavalli, S.ViswanadhaRaju, A. VinayaBabu and D.Srinivasa Kumar, "Multimodal Biometrics - Sources, Architecture & Fusion Techniques: An Overview", In proc. of IEEE International Symposium on Biometrics and Security Technologies, pp. 27-34, 2012.

[2] Muhammad Khurram Khan and Jiashu Zhang, "Multimodal face and fingerprint biometrics authentication on space-limited tokens", Neuro Computing, Vol. 17, No. 12, pp. 3026 – 3031, 2008.

[3] L.Gorman, "Comparing passwords, tokens and biometrics for user authentication," IEEE Proc., vol. 91, no.12, Dec. 2003.

[4] A.K. Jain, A Ross and S. Prabhaker, "An introduction to biometric recognition," IEEE Trans. Circuits and Systems for Video Technology, vol. 14, no. 1, pp, 4-20, Jan. 2004.

[5] Aly I. Desoky, Hesham A. Ali and NahlaB. Abdel-Hamid, "Enhancing iris recognition system performance using templates fusion", Ain Shams Engineering Journal, vol.3,pp. 133–140, 2012.

[6] S.S. Kulkarni and R.D.Rout, "Secure Biometrics: Finger Knuckle Print", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 1, no. 10, 2012

[7] V. U. Kale, R. A.Wakode and Rinky L. Batra3, "Finger Knuckle System for Human Identification: A Literature Survey ",International Journal of Emerging Technology and Advanced Engineering , Volume 5, Issue 1, January 2015)

[8] R. Szewczyk, K. Grabowski,M. Napieralska, W. Sankowski, M. Zubert, A. Napieralski, "A reliable iris recognition algorithm based on reverse biorthogonal wavelet transform", Pattern RecognitionLetters, vol. 33, no. 8, pp. 1019– 1026,2012.

[9] Acır, N., Özdamar, Ö. Güzeliş, C., "Automatic classification of auditory brainstem responses using SVM-based feature selection algorithm for threshold detection," Engineering Applications of Artificial Intelligence, Vol.19, 209-218, 2006. [10] Valentini, G., Muselli, M., Ruffino, recognition F.,"Cancer with bagged ensembles of support vector machines," Neuro computing, Vol. 56, 461-466, 2004.

[11] Zhang, Y.L., Guo, N., Du, H., Li, W.H., "Automated defect recognition of C- SAM images in IC packaging using Support Vector Machines," The International Journal of Advanced Manufacturing Technology 25, 1191-1196,2005.

[12] Karabatak, M., Ince, M.C., "An expert system for detection of breast cancer based on association rules and neural network," Expert Systems with Applications, Vol.36, pp.3465-3469, 2009.

[13] Mehmet Fatih, A., "Support vector machines combined with feature selection for breast cancer diagnosis," Expert Systems with Applications, Vol. 36, pp.3240-3247,2009.

[14]P. S. Sanjekar and J. B. Patil, "An overview of multimodal biometrics", Signal & Image Processing an International Journal (SIPIJ) Vol.4, No.1, February 2013.



[15] Wang, Y., Tan, T., Jain, A. K., "Combining face and iris biometrics for identity verification",In: Proc. of Fourth International Conference on Audio- and VideoBased Biometric Person Authentication (AVBPA). Guildford, UK, pp. 805–813, 2003.

[16] Verlinde, P., Cholet, G., "Comparing decision fusion paradigms using K-NN based classifiers, decision trees and logistic regression in a multi-modal identity verification application", In: Proc. of Second International Conference on Audioand Video-Based Biometric Person Authentication (AVBPA). Washington, DC, USA, pp. 188– 193, 1999.

[17] Chatzis, V., Bors, A.G., Pitas, I., "Multimodal decision-level fusion for person Authentication", IEEE Trans. Systems Man Cybern. Part A: Systems Humans, vol 29, no.6, pp.674–681, 1999.

[18] Fahmy, M.S., Atyia, A.F., Elfouly, R.S., 2008. Biometric fusion using enhanced SVM classification. In: 2008-Fourth International Conference on Intelligent Information Hiding And Multimedia Signal Processing. Harbin, pp. 1043–1048.

[19] Park, H.A., Park, K.R., "Iris recognition based on score level fusion by using SVM", Pattern Recognition Letter, vol. 28, no.15, pp. 2019–2028, 2007.

[20]MadasuHanmandlu ,Jyotsana Grover, AnkitGureja and H.M. Gupta, "Score level fusion of multimodal biometrics using triangular norms", Pattern Recognition Letters, vol. 32, pp.1843–1850,2011

[21] Swathi S. Dhage, SushmaShridharHegde,

K. Manikantan and S. Ramachandran, "DWT-1. 41, no. 3, pp. 805-813 , 2008. International Journal of Research in Management, Science and Technology

Feature Extraction based and Radon Transform Based Contrast Enhancement for Improved Iris Recognition", Procedia Computer Science, vol.45, pp.256-265, 2015. [22] Lan LIN, Ge ZHAO, Yan-Dong TANG, Jian-Dong TIAN and Si-Yuan HE. "Illumination Compensation for Face Recognition Using Only One Image", ActaAutomaticaSinica, vol. 39, no. 12, pp. 2090-2099, 2013.

[23] Patricia Melin, Daniela Sanchez and Oscar Castillo, "Genetic optimization of modular neural networks with fuzzy response integration for human recognition"

Information Sciences, pp.1-19, vol.197, 2012

[24] Shoichiro Aoyama, Koichi Ito and Takafumi Aoki, "A finger-knuckle-print recognition algorithm using phase-based local block matching", Information Sciences, vol.268, pp. 53-64, 2014.

[25] JialiangPeng, Ahmed A. Abd El-Latif, Qiong Li and XiamuNiu, "Multimodal biometric authentication based on score level fusion of finger biometrics", International Journal for Light and Electron Optics, vol. 125, no. 23, pp. 6891-6897, 2014.

[26] Muhammad Khurram Khan and Jiashu Zhang, "Multimodal face and fingerprint biometrics authentication on space-limited tokens", Neurocomputing, vol. 71, pp. 3026-3031, August 2008.

[27] T. Zhang, X. Li, D. Tao, and J. Yang, "Multi-modal biometrics using geometry preserving projections", Pattern Recognition, vo