A Proposed Algorithms to Design Support Multimodal biometric System

Hanaa M. Ahmed*,Ph.D (Asst. Prof.) Bushra J. Abdulkareem**

Abstract

This paper is an attempt to address the biometric security issue and improve the system accuracy through introducing a design for multimodal biometric verification system using multiple traits (Iris, fingerprint) and adding another phase called liveness detection to the phases of multimodal system the purpose of this phase is to protect the multimodal biometric systems against spoofing attacks. The system is tested in two levels, unimodal level and multimodal level (fusion level). in unimodal level two tests have been performed, one for iris verification phase performed on two types of database MMU DB (Multi Media University database) for 180 samples and CASIA DB (Chinese Academy of Sciences database) for 90 samples. and gave accuracy (99.44%) with FAR (False Acceptance Rate) of (0.0277) and FRR (False Reject Rate) (0.0055) for MMU DB, and accuracy (97.77%) with FAR of (0.0333) and FRR (0.0222) for CASIA DB, and other for fingerprint verification phase performed on database collected from two types of database for 60 samples and gives accuracy of 95% with FAR of 0.1% and FRR of 0.05%.

In multimodal level the system is tested on database composed of 60 samples for iris images and 60 samples for fingerprint images and gives an overall accuracy of 100% with FRR of 0%, and FAR of 0.0166%.

Keywords: Liveness detection, Multimodal, Iris, Fingerprint, Anti-spoofing, Verification, Fusion function.

*University of Technology

**Al-Mansour university College

1. Introduction

Reliable verification schemes is require in wide variety of applications such as secure access to buildings, computer systems, laptops, cellular phones and ATMs, to confirm the identity of an individual requesting their service. Unimodal biometric systems establish person verification based on a single biometric trait, its characteristic needs to meet some basic requirements like [1 and 2]: Universality, Uniqueness, Permanence, and Collectability. However, there are a number of other issues that should be considered with any biometric trait that meets previous criteria, these are, Performance, Acceptability, and Circumvention.

From the practical applications, no biometric characteristic fully meets these requisites. Besides it suffers from noisy sensor data, poor quality biometric traits, continuous threats of spoof attacks, and unacceptable error rates etc., hence, may not always meet crucial security requirements. Multimodal biometric systems that consolidate evidence from multiple biometric sources can be used to overcome or minimized some of these limitations [3 and 4].

Many previous researches addressed the issue of “anti-spoofing” in unimodal biometric systems, the common method used for this purpose, is to insert an additional module, called “liveness detector” that is used as a countermeasure to spoof attacks to assess if an input biometric sample acquired by some sensors belongs to a “live” person or is a “spoof” artifact [6].

Anti-spoofing in multimodal biometric systems, is not a clear concept as in the unimodal case. Multimodal biometric systems have been commonly believed to be intrinsically more robust to spoof attacks than unimodal systems. This confidence is based on the intuitive hypothesis that evading the multimodal biometric system always requires an attacker to spoof all the involved traits (or at least more than one). Recently this belief has been questioned and several works provided clear evidence that they can be evaded by spoofing a single biometric trait, as in [3, 6, 7, and 8]. These researches showed that number of vulnerability points will be increased in multimodal biometric system, and can be explored by an

intruder. Hence a multimodal system may be easier to spoof than some of the unimodal systems that compose it. This question is especially important when multimodal system combining face traits which can be easily spoofed, and retina veins traits which is very hard (if not impossible) to spoof. In this case, an impostor that spoofs only the face trait may have a very high chance of being falsely accepted [3 and 7].

This paper is an attempt to address the biometric security issue and improve the system accuracy through introducing a design for multimodal biometric verification system using multiple traits (Iris, fingerprint) and adding another phase called liveness detection to the phases of multimodal system to protect the multimodal biometric systems against spoof attacks.

2. Literature Survey

As any of the traditional security systems, identity verification systems that use biometric, attempts to attack him by opponents, and who have the ability to compromising data integrity through alteration so the system becomes inactive. Many researchers and designers of biometric systems highlighted the lack of security in regards to biometric systems through the provision of studies and algorithms to solve this issue. Therefore, the evaluation of these systems is an open question whether the investigation will lead to a secure biometric systems design [5]. To build secure biometric systems it is necessary to understand and evaluate these threats through the development countermeasures, design of impervious against these attacks. Many researchers who study the weaknesses in the biometric systems, possible attack methods and their countermeasure, here is a collection of previous studies related to the paper theme:

In 2009, R. N. Rodrigues, L. L Ling, and V. Govindaraju [3] Propose two original multi-modal biometric fusion's methods that consider the spoofing assumptions and the security of each uni-modal biometric being merged. One method which is an extension of the Likelihood Ratio (LLR), and the other method, is using fuzzy logic. The

two models follow the same basic ideas, but their details and implementation are different. The work in these two schemes shows that when using traditional fusion method (i.e. weighted sum or LLR) attacker's chances of evading a multi-modal system by spoofing only one of the biometrics can dramatically increase. Experiments showed, first: the existence of a trade-off between robustness against spoof attacks, and recognition accuracy, second: the fuzzy fusion scheme had a best overall performance compared with the probabilistic fusion scheme.

In 2011, Maruf Monwar et al. [4] Rreliable and robust multi-modal biometric based security system have been proposed, it composed of (face, ear, and iris) and use soft biometric identifiers (gender, ethnicity and eye color). A novel fuzzy fusion technology is used to fuse these biometric traits. This scheme adopts match score, rank information and soft biometrics information from unimodal biometrics as the input, and final identification decision via a fuzzy rule as output. Supplement information about the identity of a subject has been provided by their research that makes the operation of human recognition more accurate. The improvement in recognition performance results is duo to the used of an optimum weighting scheme has been advanced based on the distinctive abilities of the primary and the soft biometric traits. Comparison for the experimental results between the fuzzy fusion technology and other fusion methods has been conducted, which prove that the proposed method is not only accurate but also faster beyond existing technologies.

In 2012, P.U.Lahane, and S.R.Ganorkar [9] suggested Multimodal biometric identification system, composed of (iris and fingerprint). Each biometric trait processes its information independently. In this system, the iris is extracted, removes the influence of the eyelids and eyelashes, and through a series of operations on the eye image provided. Singularity region is segmented from input fingerprint image by preprocessing operations performed on it. Then the Region of Interests (ROI) extracted and used as input for the normalization. Gabor filter used to extract features from fingerprint and iris. Then fusion is performed in the feature

extraction level by combining the biometric features extracted from fingerprints and irises images. Finally Euclidean Distance is the matching algorithm used for computing matching score. Experimental threshold used to decide whether or not the two representations belong to the same user by comparing with the result of the measurement. This work produces efficient security system**.**

In 2012, Akhtar Z, Fumera G, Marcialis GL and Roli F, [11] this research presented "comparison based robustness against spoofing attacks between serial fusion of multi-modal systems, and parallel multi-modal systems, by empirically analyzing between the robustness of serial fusion of dual modal systems with the corresponding parallel systems, using of a fingerprint and a face matcher, against several real spoofing attacks. Results obtained regarding the level of fusion rules, which were common in the literature, are not robust to spoofing attacks as believed, since they can be avoidable by spoofing only one biometric trait. Also, spoofing the extremely accurate biometrics makes more probably to avoid a multi-modal system. However, they found confirmations that serial multi-modal systems are more robust than parallel ones versus spoofing attacks, and can earn a better trade-off between performance, verification time, user acceptability and robustness.

In 2013, Dapinder and Gaganpreet [10] Stated the fusion methods by dividing it into the following three categories:(max, or, product, majority voting, min, sum, and) belong to first category (fixed rule-based methods), and (the Bayesian inference, support vector machine, maximum entropy model, and neural networks) belong to the second category (classification based methods), and the third category (estimation-based methods) which includes (the particle filter fusion methods, Kalman filter, and extended Kalman filter). These methods have been primarily used to better estimate the state of a moving object based on multimodal data. The basic nature of these methods is the base of this categorization, and it means the classification of the problem scope, such as, estimation-based methods solved a problem of

estimating parameters. And classification-based or rule based methods solved the problem of obtaining a decision based on specific observation.

3. Individual Recognizers

Iris and fingerprint biometrics perform better as compared to other available traits due to their accuracy, reliability and simplicity. These properties make iris and fingerprint recognition particularly promising solution to the society. Below is theoretical part of these two biometric traits and the method used for fused these traits**.**

3.1 Iris Recognition

Iris is an important feature of the human body and unique to each individual and very stable throughout lifetime of a person. Iris biometric trait offers many advantages over other human biometric features. The Iris is the only internal human body organ that is visible from the outside and is well protected from external modifiers. Due to the richness of the texture details in the iris image the eyes of an individual contain completely independent iris patterns, and these minute details are randomly distributed which make the human iris as one of the most important biometric characteristics [12].

3.2 Fingerprint Recognition

Fingerprints are one of the most widely used biometric modality which used in courts of law in all over the world. And increase number of civilian and commercial applications which used fingerprint-based identification, because of their three properties. First the character of the pattern on each finger is permanent and unchanged, second the ridge details are uniqueness ,and the third point is the feature vector can be easily extracted from fingerprint and stored in a compact fashion, and suitable for matching [2 and 13].

3.3 Fusion

Fusion is the procedure which performs integrates information from multiple biometric traits to consolidate the effectiveness of the biometric system and making it difficult for an intruder to spoof multiple biometric traits simultaneously. In this proposed system the fusion is performed in the matching score level, after the extraction of the features of each model in the multi-modal system, matching the stored data, and test data for each biometric feature using the same matching algorithm. Scores generated from matching module from each biometric trait moved to score fusion rule at matching score level using weighted sum of fusion technique. In Fusion: The two resulted scores Na and Nb are fused linearly using weighting sum rule as [14]:

$$MS=\alpha X\, N_a + \beta X N_{b,} \qquad \dots (1)$$

Where (αX) and (βX) are two weight values that can be determine by the training data which considered the degrees of accuracy for each biometric trait contributed to construct the system.

3.4 Performance Measures used in Biometric System

The fundamental parameters used to measure the performance of biometric verification systems are explained below:

1. **False Acceptance Rate (FAR):**
   It measures the likelihood of confusing two identities or it is the ratio of acceptance intruder falsely. Obviously, this measure very affected by the desirable security degree and the system goodness.FAR can be defined as [15]:

$$FAR = \frac{Number\ of\ times\ different\ person\ matching \times 100}{Number\ of\ comparison\ between\ difference\ persons} \quad \dots(2)$$

2. **False Reject Rate (FRR)**
   It measures the probability that enrolled person is identified wrongly; in other word it is the rate of rejecting real user. FRR can be defined as:

$$FRR = \frac{Number\ of\ times\ same\ person\ rejected \times 100}{Number\ of\ comparison\ between\ same\ persons} \quad \ldots(3)$$

4. The Proposed System

This proposed system has been constructed by using multimodal schema represented by iris and fingerprint models. The steps of the proposed system are shown in figure (1):

Algorithm (1): multimodal system
Input: 1- Two samples of eye images 2- Two samples of fingerprint images **Output** : Final decision, if person has been genuine or imposter or it is fake try
Begin **Step 1**: Read the two samples of eye image **Step 2:** Execute dynamic liveness detection module on the two samples of eye image to cheek liveness. If the result from this module true then goes to (step3) otherwise make the decision (the request is fake) and go to end. **Step 3:** one of the two samples of eye image input to the static liveness detection module. If the result from this module is true go to (step 4) otherwise make the decision (the request is fake) and go to end. **Step 4:** read two samples of fingerprint image **Step 5:** Cheek dynamic liveness for the two finger image if result from this module is true go to step 6 otherwise make the decision (the request is fake) and go to end. **Step 6:** one of the two samples of fingerprint image input to the static liveness detection module. If the result from this module is true go to (step 7) otherwise make the decision (the request is fake) and go to end. **Step 7**: perform iris verification module in this module feature vector is extracted and comparison is performed between the feature vector submitted by the person and the one stored in its database called (template) to produce iris matching score. **Step 8**: Fingerprint verification module are executed by extract feature vector and compute fingerprint matching score

Step 9: Fusion for the matching scores result from (step 7) and (step 8) are performed using weighting sum rule
Step 10: make the final decision according the result from (step 9) if the result is equal or greater than (85) then the person is genuine else the person is imposter.
End Algorithm

Figure (1) The algorithm of the proposed system

The algorithm start with very important phase called liveness detection in both (static sub model and dynamic sub model) for each one of those two models, which added to the system to protect it from spoof attack. And then verification phase to produce matching scores from two biometric traits iris and fingerprint. And the last phase in proposed system which represent by fusion phase where a person is declared as genuine or an imposter as following: Figure (2) illustrates the architecture of the proposed system.

4.1 Liveness Detection Phase

In iris liveness detection module two modules used to detect liveness. The variation in pupil size caused by acquired eye images for the same person in different lightness which is restricted in the range (5-15%) is exploited to detect the liveness in input eye image by dynamic iris liveness detection module. In static iris liveness detection module the property of focus degree of the acquired eye image by compute the sharpening of eye image using high pass filter used to detect liveness in input eye image. The threshold detecting by training data in this algorithm to make liveness decision is (34) (if the mean of gradients of eye image less than 34 then the input image sample is fake else it is live). In fingerprint model also two module used to detect liveness, Dynamic module by compute difference in standard deviation between two input fingerprint image acquired in period of time (3-5 second), and static module by using number of First order statistical features, and properties extracted from analyze input fingerprint image. The output from liveness detection phase decides whether the acquired image come from real or fake biometric trait. If the decision that the acquired image come from fake biometric trait, from any one of two models (iris or fingerprint), the

processing operation will be stopped, and the system points that this request to enter to the system is spoof attack. Else if the decision that the acquired images come from real biometric traits, the algorithm will be continue and moves to verification phase.

4.2 Verification Phase

This phase composed of two modules for produce matching scores executed in parallel one for iris verification model and other for fingerprint verification model. Below is the explanation for these two models:-

4.2.1 Iris Verification Model

The iris verification module work as following:

The eye image of the user who claims his identity is input to the iris verification module and pass through sequence of steps started with iris segmentation which performed by, pupil localization which done through eight point ending with compute the radius Rp and center coordinates (Cpx,Cpy) of the pupil to detect the inner boundary. And then iris localization to detect the outer boundary which performed by produce the gradient image using canny edge detector, and then using circular summation by exploit pupil's radius and center coordinates of the pupil. Summing the intensities over all circles, pass over all possible radii starting from pupil's radius +15 to the pupil's radius + 50 and center coordinates of the pupil . The circle with highest summation corresponds to the outer boundary. After this the interest region will be detected by selecting the part of iris region to the left and right and to the bottom of the pupil; selection the region in this way is to avoid noise caused by eyelashes and eyelids, then made all gray level values in pupil region equal to zero to isolate it from selected region. The feature vector will be extracted from this region using series of second order statistical feature computed from GLCM for this region. In the matching, these feature set compared with the enrolled respective feature vector stored in the database (template) of the claimed identity using (percentage of the matching) algorithm to produce the iris matching score.

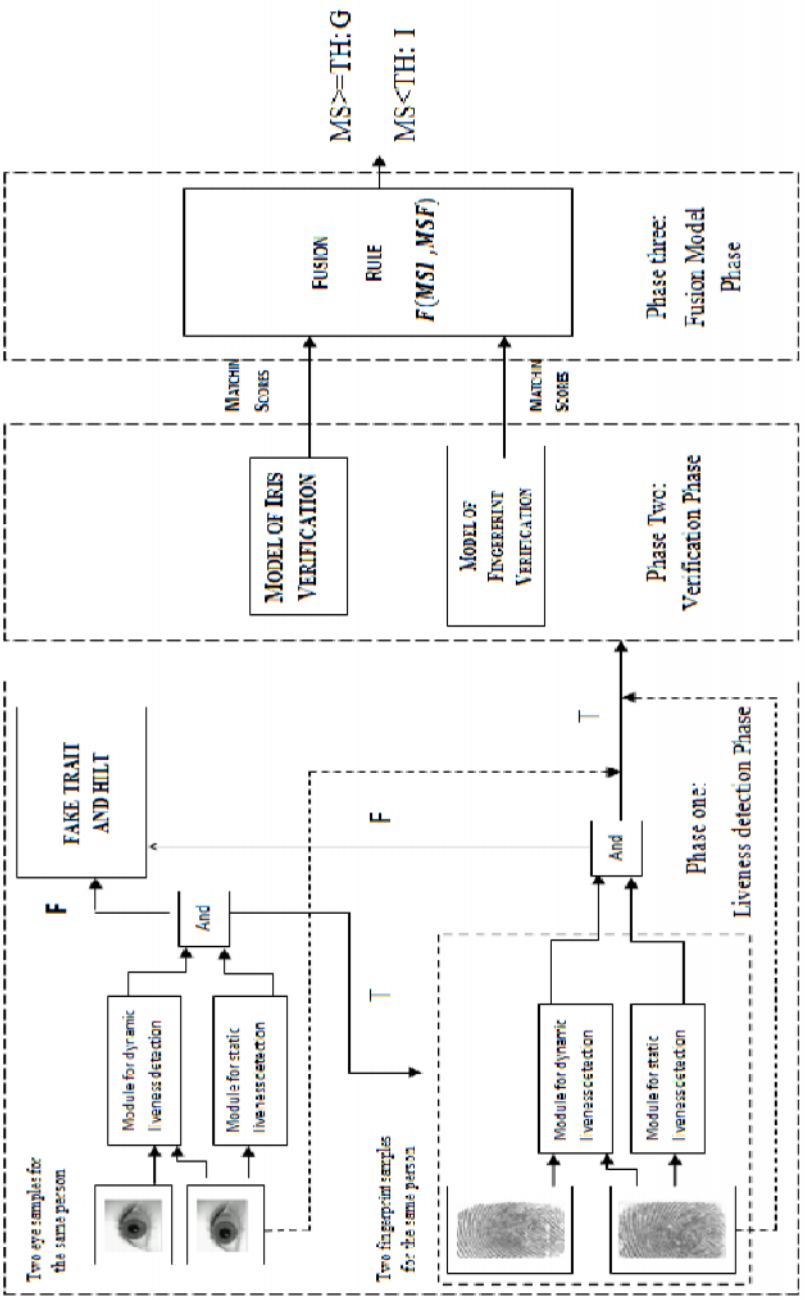

Figure (2): The architecture of the proposed multimodal system

4.2.2 Fingerprint Verification Model

In the other side of the proposed system, the fingerprint image for the same user input to the fingerprint verification module which pass through preprocessing operation include: first remove noise by adaptive filter, second segment the image, third binarization the segmented image, last thinning this binary image. Feature vector will be extracted from thinning image using central moment technique. The same operation performed in the iris matching will be performed in the fingerprint matching, to produce fingerprint matching score result.

4.3 Fusion Phase

The matching scores produced from phase two for two biometric model (iris and fingerprint) have been input to the phase three of the system to be linearly fused by using weighting sum rule illustrated in equation (1).

Where α, and β are weight values that determined by the training data which consider the degree of accuracy for each biometric traits contributed to construct the system. T is threshold previously defined. Hence if the Fused Score (FS) $\geq$T, then user is accepted as Genuine (G), otherwise it is rejected as an Impostor (I).

5. Experiment Result

To show the benefit of designing multimodal biometric system, the experiment results will be presented in two levels. These levels are liveness detection and verification.

5.1 Liveness Detection Results

The first level of experimental results is liveness detection. In this level two field of experiment have been illustrated, these are iris liveness detection and fingerprint detection:

5.1.1 Iris liveness detection module:

Database that is set up to test the robustness of the proposed system through iris liveness detection process consists of 15 original (***MMU database)*** [16] folders ***each*** folder contain two eye image samples represent live tries, and 15 (***MMU database)*** folders of eye images printed using scanner devise and recapture using specific camera and

resaved in computer to represent 15 attempted spoof attack against the system. Each folder contained two samples of fake eye image. Table (1) show experiment results for dynamic iris liveness module and Table (2) show the results of static iris liveness module:

Table (1): The experiment results for dynamic iris liveness module

	Results by Appling on original eye images			Results by Appling on recaptured eye images		
Person No.	No. of pixel in pupil for two samples with different eliminations	Percentage Difference in pupil size	decision	No of pixel in pupil for two samples with different eliminations	Percentage Difference in pupil size	decision
1	291210 325125	11.005	Live	694620 695895	0.183	Fake
2	482460 540090	11.272	=	682380 691050	1.613	Fake
3	457980 525300	13.693	=	1418310 1419330	0.072	Fake
4	330735 372300	11.824	=	961605 974355	1.317	=
5	699210 759900	8.319	=	512295 772395	40.492	=
6	410550 474300	14.409	=	930495 759900	20.184	=
7	408000 431460	5.589	=	1266075 1327530	4.739	=
8	337875 368220	8.595	=	542640 548760	1.121	=
9	248625 288150	11.116	=	482715 685695	34.745	=
10	514845 566355	9.528	=	675750 907800	29.308	=
11	585735 627555	6.894	=	1564425 1195695	26.718	=
12	469455 536010	13.239	=	828750 562785	38.226	=
13	439110 469710	6.734	=	1036065 1171980	12.311	faulty live
14	336345 336345	5.529	=	818805 842265	2.825	Fake
15	719865 762450	5.746	=	1002915 860880	15.241	Fake

Table (2) the experiment results for static iris liveness module

	Results by Appling static module on original eye images		Results by Appling static module on recaptured eye images	
Person No	Mean of gradient for input original MMU eye sample images	decision	Mean of gradient for input recaptured MMU eye sample images(spoof image)	decision
1	45.867 38.969	Live =	28.808 32.486	Fake =
2	36..203 58.622	Live =	29.355 39.577	Fake Faulty Live
3	42.561 37.927	Live =	34.55 30.977	Faulty Live Fake
4	35.306 35.998	Live	29.382 28.72	Fake =
5	55.638 49.592	Live =	32.273 32.884	= =
6	36.935 41.593	Live =	26.155 28.721	= =
7	36.489 36.454	Live	27.464 29.281	= =
8	35.789 45.489	Live	26.947 32.051	= =
9	35.49 35.186	Live =	26.22 25.554	= =
10	35.511 34.5	Live =	27.708 23.303	= =
11	35.122 35.052	Live =	25.392 28.361	= =
12	39.363 37.276	Live =	28.55 28.323	= =
13	36.702 38.173	Live =	23.235 28.416	= =
14	34.363 35.389	Live =	23.112 27.843	= =
15	35.55 33.55	Live =	26.295 24.792	= =

5.1.2 Fingerprint liveness detection results:

Database that is set up to test the robustness of the proposed system through fingerprint liveness detection process consists of 12 folders of original fingerprint database Each folder contain two fingerprint images sample represent live tries, 12 folders generated from original database used in verification phase to represent fake tries. Table (3) show experiment results for dynamic fingerprint liveness module and table (4) show the results of static fingerprint liveness module.

Table (3) The experiment results for dynamic fingerprint liveness module

	Results by Appling on live fingerprint samples			**Results by Appling on fake fingerprint samples**		
Person No	**Standard deviation for two input samples computed based on GLCM normalized matrix**	**Percentage Difference in two standard**	**decision**	**Standard deviation for two input samples**	**Percentage Difference in two standard**	**decision**
1	0.788 0.725	8.333	Live	0.763 0.788	3.209	Fake
2	0.732 0.78	6.418	=	0.817 0.786	3.884	Fake
3	0.525 0.411	24.319	=	0.525 0.513	2.394	Fake
4	0.855 0.668	24.584	=	0.655 0.668	2.02	=
5	0.706 0.757	6.997	=	0.758 0.799	5.447	faulty live
6	0.701 0.802	13.556	=	0.58 0.58	0	Fake
7	0.743 0.851	13.521	=	1.232 1.243	0.838	=
8	0.829 0.769	7.405	=	0.829 0.809	2.412	=
9	1.306 1.501	13.919	=	1.477 1.501	1.668	=
10	1.006 1.495	39.101	=	1.006 1.007	0.105	=
11	1.418 1.278	10.4	=	1.418 1.456	2.647	=
12	1.869 1.681	10.653	=	1.936 1.871	3.399	=

Table (4) the experiment results for static fingerprint liveness module

No.	Original/captured	Rao1	Rao2	mean	Energy	variance	Kurtosis
1.	Original	14.694245	0.0004947	2.005844	5469.826	21870917.77	0.002067
	Captured	0	0	1.4218	2455.869	2274110.788	0.00322
2.	Original	6.31323490	0.1907496	1.49317	5100.496	16832942.407	0.00291
	Captured	0	0	1.4218	1921.318	2054730.515	0.00354
3.	Original	26.155145	7.4634910	1.840148	4112.509	19312355.021	0.00224
	Captured	0	0	1.4218	2377.84	1514958.28	0.00338
4.	Original	2.9797069	0.00030003	1.678756	2754.41	15374683.366	0.002785
	Captured	0	0	1.4218	1767.457	1748983.244	0.0038460
5.	Original	0.478353	0.563804	1.421875	30618.22	13840099.733	0.003754
	Captured	0	0	1.4218	2107.362	2377095.068	.0045012
6.	Original	5.6075581	.20576589	1.421875	24902.71	16718770.69	0.003090
	Captured	0	0	1.421875	1.421875	3002221.079	0.003486
7.	Original	1.4583712	6.1065050	4.6875	1065839.9	69272205.80	0.000881
	Captured	0	0	1.421875	4784.820	2516529.38	0.003273
8.	Original	0.526416	3.656012	4.6875	885777.3	63127761.85	0.000964
	Captured	0	0	1.421875	3045.649	3140497.75	0.004039
9.	Original	0.607280	0.359060	1.421875	20955.06	12589930.35	0.003897
	Captured	2.14633E-05	0	1.421875	1628.664	2819894.415	0.004536
10.	Original	0.341605	0.412820	1.421875	30254.21	12531497.963	0.003869
	Captured	0	0	1.421875	2154.626	2221829.152	0.004986
11.	Original	0.011108	0.003	0.3973388	104.1590	1013907.64	0.013428
	Captured	0.0053482	0.0010496	0.39733	97.0417	1048356.372	0.015515

5.2 Verification Results

The second level of experimental result is verification. In this level three folds of experiment have been illustrated. These are, iris verification model, fingerprint verification module, and finally fusion module.

5.2.1 Iris verification Experimental Results

Two types of iris database used to training and testing the proposed system, these are: ***MMU Iris database and CASIA-IrisV1database*** [17]***.*** The training of iris verification algorithm consists of three experiments as follow:

The first experiment conducted to test of the proposed iris verification algorithm by applied on 180 eye image of ***MMU database*** for 30 persons for left and right eyes. Three samples for left eye and three sample for right eye for each person. The second experiment testing of the proposed iris verification algorithm phase by applied on 90 image of ***CASIA-IrisV1 database*** for 30 persons. Three samples of eye image ***for each person.*** In the third experiment the eye images database collected for testing the proposed multimodal verification algorithm as completed system. Started from liveness detection phase and ending with fusion phase consists of 15 folders of (MMU database) for 15 person each folder contained four samples for left eye image. Table (5) clarify the results of testing operation for verification phase of iris model and the accuracy computed and The FAR and FRR.

Table (5) experiment results of the iris verification phase

Eye image Database	No of people	No. of samples	No. of samples successfully verification	No. of samples faulty accepted	No. of samples faulty rejected	Tame of verification	Time for matching	FRR %	FAR%	Average accuracy
MMU DB	30	180	179	5	1	20 second	0.8 second	0.0055	0.0277	99.44%
MMU DB	15	60	59	2	1	20 second	0.8 second	0.0166	0.0333	98.33%
CASIA (Version 1.0)	30	90	88	3	2	24 second	0.8 second	0,0222	0.0333	97.77%

5.2.2 Fingerprint Verification Experimental Results

The database collected for training and testing fingerprint verification model is consists of 15 folders for 15 persons each folder contain four fingerprint image samples for same person. The database taken by the internet from the database of University of Bologna and all of them are gray scale of a tiff image file format. The results of testing operation for verification phase of fingerprint model are showed in table (6) which illustrates the accuracy and FAR and FRR.

Table (6) experiment results of the fingerprint verification phase

fingerprint image Database	No. of people	No. of samples	No. of samples successfully verification	No. of samples faulty accepted	No of samples faulty rejected	Tame of verification in seconds	Time for matching in seconds	FRR %	FAR %	Average Accuracy
University of Bologna	15	60	57	6	3	24	0.8	0.05	0.1	95

6.Fusion Experimental Results

In this fold of experiment result the matching scores of the iris and fingerprint are combined and total accuracy is computed, as shown in Table (7). The combination of two databases, Iris database which composed of 15 folders as maintained in iris verification phase, and fingerprint database which is the same database used in fingerprint verification phase used for whole system which ending by fusion phase.

From the accuracy results showed previously in iris verification phase and fingerprint verification phase, the accuracy of iris verification is highest than the accuracy of fingerprint verification, on this basis, the values of (α = 0.7 : which represent the weight given to iris matching score) and (β= 0.3 :which represent the weight given to fingerprint matching score) and perform fusion operation by apply fusion equation.

Table (7) experiment results of (fusion phase)

Data set used	No of people	No of matching scores	No of fusion operations	No of fusion successfully verification	Tame of verification For complete system in seconds	Time for fusion operation in seconds	Average accuracy
MMU iris database and University of Bologna for fingerprint	15	60 for iris 60 for fingerprint	60	60	45.5	0.5	100%

Table (8) shows the accuracy obtained of unimodal and combined system. The whole performance of the system has increased in multimodal production accuracy of 100% with FAR of 0% and FRR of 0% consecutive receivers.

Table (8) experiment results iris and fingerprint (fusion phase)

Biometric verification module	Database used	No of person	No of verification operation	No of successfully verification operation	Time for verification operation in seconds	Average accuracy
Iris verification	MMU	15	60	59	20	98.33%
Fingerprint verification	University of Bologna	15	60	57	25	95%
Multimodal iris and fingerprint verification system	MMU and University of Bologna	15	60	60	45.5	100%

The accuracy result of proposed system is compared with the accuracy results of other existing methods. This comparison are showed in table (9)

Table (9) experiment results of the proposed system and other existing system accuracies.

Author	Biometric system	Database	Algorithm	FAR	FRR	accuracy
Hunny, Ajita, Phalguni	Multimodal (iris, fingerprint)	database collected by the authors for 200 samples	Haar + Minutiae	1.58	6.43	96.04%
P.U.Lahane, Prof. S.R.Ganorkar	Multimodal (Iris + Fingerprint)	ten users with five iris image & five Fingerprint image of each person	Gabor filter	0.3	0.5	99.5
Proposed algorithm	Multimodal (Iris + Fingerprint)	fifteen users with four iris image & four Fingerprint image of each person	Second order statistical feature and central moment features	0.0166	0	100%

7. Conclusions

By extensive and hard work in the design of the proposed system which composed of multimodal biometric system to improve the security and accuracy of these types of system through adding another module (liveness detection) to it, number of conclusions have been reached:-

1. The dynamic method which used to detect liveness is more effective, more accuracy and success than static method. Static method need to detect fixed threshold, extracted from original properties of the biometric trait to accept image sample as real sample. Choosing this threshold be influenced by the variance of these original properties from person to another, such as degree of sharpening of eye image and the first order statistical features which extracted from fingerprint image. And the way used to collect the original image database and manufacture spoof database which is, cause ratio of error in liveness decision.
2. in matching module of this proposed system there is a specific percentage rate (0.1) for similarity between each element in test feature vector with corresponding element in template feature vector allowed to it to enter into the comparison process to produce the final matching score , this to avoid FAR in this system.
3. In biometric verification system, multimodal is better, and more accuracy than single model, because the biometric traits for these two model (iris and fingerprint) are fused using specific fusion function, through merge matching score coming from fingerprint based on invariants central moment feature and iris matching score based on radius of pupil and second texture feature from the normalized GLCM, and consider the degree of accuracy of these two models.

References

[1] Mohamed Soltane , Mimen Bakhti, " Multi-Modal Biometric Authentications: Concept Issues and Applications Strategies" , International Journal of Advanced Science and Technology, Vol. 48, November, 2012.

[2] Ebtesam Najim AL_Shimmary, "Fingerprint Image Enhancement and Recognition Algorithms", Ph.D thesis, University of Technology, May, 2007.

[3]. R. N. Rodrigues, L. L Ling, and V. Govindaraju," Robustness of multimodal biometric fusion methods against spoof attacks", Journal of Visual Languages and Computing, Vol. (20), Issue (3), June, 2009.

[4]. Md. Maruf Monwar, Marina Gavrilova, " *A Novel Fuzzy Multimodal Information Fusion Technology for Human Biometric Traits Identification*",IEEE, International Conference on biometric compendium , 20 Aug. 2011

[5]. Marta GomezBarrero, Javier Galbally, Julian Fierrez , Javier OrtegaGarcia, "Progress in Pattern Recognition, Image Analysis, Computer Vision, and Applications", Springer Berlin Heidelberg, November, 2013.

[6]. Giorgio Fumera, Gian Luca Marcialis, Battista Biggio, Fabio Roli and Stephanie Caswell Schuckers, "Handbook of Biometric Anti-spoofing" , Springer London, July 2014.

[7]. P. A. Johnson, B. Tan, S. Schuckers, "Multimodal Fusion Vulnerability to Non-Zero Effort (Spoof) Imposters, IEEE International workshop on information, December, 2010.

[8]. Ricardo N. Rodrigues, Niranjan Kamat and Venu Govindaraju, "Evaluation of Biometric Spoofing in a Multimodal System", IEEE International Conference on biometric compendium, Sept. 2010

[9]. P.U.Lahane, Prof. S.R.Ganorkar, “Fusion of Iris & Fingerprint Biometric for Security Purpose", International Journal of Scientific & Engineering Research Volume 3, Issue 8, August-2012.

[10]. Marfella L, Marasco E, Sansone C, “Liveness-Based Fusion pproaches in Multibiometrics", IEEE International workshop, Sept. 2012.

[11]. Akhtar Z, Fumera G, Marcialis GL, Roli F, "Evaluation of serial and parallel multibiometric systems under spoofing attacks" In: Proc. IEEE Fifth International Conference on biometric compendium. Washington DC, USA, Sept. 2012.

[12]. Babasaheb G. Patil, Shaila Subbaraman, “SVD-EBP Algorithm for Iris Patten Recognition”, International Journal of Advanced Computer Science and Applications, Vol. 2, No. 12, 2011.

[13]. M.Mani Roja, Sudhir Sawarkar, Ph.D, " Fingerprint Verification System – A Fusion Approach", published in International Journal of Computer Application (IJCA), 2011.

[14]. Battista Biggio, Zahid Akhtar, Giorgio Fumera, Gian Luca Marcialis, and Fabio Roli, "Security Evaluation of Biometric Authentication Systems Under Real Spoofing Attacks ", IEEE, Biometrics compendium, Volume:1 , Issue: 1, march, 2012.

[15]. Rajesh M. Bodade, Sanjay N. Talbar, " *Iris Analysis for Biometric Recognition Systems*", Springer, 2014.

[16]. MMU1: http://pesona.mmu.edu.my/~ccteo/.
[17]. CASIA V1 :http://biometrics.idealtest.org/dbDetailForUser.do?id=1

اقتراح خوارزميات لتصميم نظام حصين متعدد الوسائط للتعرف على الهوية الشخصية

أ.م.د.هناء محسن احمد* بشرى جبار عبدالكريم **

المستخلص

هذا البحث هي محاولة لمعالجة امن انظمة التحقق من الهوية الحيوي ولتحسين دقة النظام بتقديم تصميم لنظام التحقق متعدد الوسائط باستخدام ميزات متعددة (قزحية العين وبصمة الاصبع) واضافة مرحلة اخرى تدعى مرحلة تحديد الحيوية (Liveness Detection) الى مراحل النظام المتعدد لحماية نظام التحقق من الهوية الحيوي المتعددة الوسائط من هجمات الاختراق بالتحايل.

أُختبرت كفاءة التحقق للنظام في مستويين، المستوى الاحادي الوسائط والمستوى المتعدد الوسائط. إذ أُختبر النظام ضمن المستوى الاحادي باستخدام قزحية العين ولنوعين من قواعد البيانات قاعدة بيانات جامعة الوسائط المتعددة (MMU DB) وكان عددها 180 عينة لـ 30 شخصاً، وقاعدة بيانات الاكاديمية الصينية (CASIA DB) كان عددها 90 عينة لـ 30 شخصاً. وأعطى دقة (99.44٪) مع FAR (0.0277) وFRR (0.0055) للMMU DB، ودقة (97.77٪) مع FAR (0.0333) و FRR (0.0222) للCASIA DB، والاختبار الآخر ضمن المستوى الاحادي للتحقق من الشخص عن طريق البصمة التي أجريت على قاعدة البيانات تتكون من 60 عينة لـ 15 شخصا ومنحت دقة 95٪ مع FAR (0.1%) و FRR (0.05%) .

اختبر النظام في مستوى المتعدد الوسائط على قاعدة بيانات تتكون من 60 عينة لصور قزحية العين و60 عينة لصور بصمة اصبع وقد وصلت دقة النظام حسب نتائج الاختبار الى 100%مع FAR (0.0166) و FRR (0%).

الكلمات المفتاحية: تحديد الحيوية، المتعدد الوسائط، قزحية العين، بصمة الاصبع، اثبات الهوية، دالة الاندماج.

* الجامعة التكنولوجية

** كلية المنصور الجامعة