

INTEGRATING FACE RECOGNITION ALGORITHMS WITH TYPING SPEED FOR WEBSITE AUTHENTICATION

MOHAMAD AMIR DLIWATI* & DR. MUHAMMAD MAZEN ALMUSTAFA**

Department of Web Sciences, Syrian Virtual University, Syria

Email: mohamed_amir_58826@svuonline.org *, t_mmustafa@svuonline.org *

ABSTRACT

Website authentication has started and developed in 1995. When people started to use the internet for shopping, sending emails, managing account, etc... Internet plays a basic role in every in life's domain people use it in different ways. Meanwhile the usage of the internet was monopolized for the educated people and the industrialists whom used it to send emails or to do researches that support their own queries. Developing the applications and the projects that depend on the internet went simultaneously with the development of hacking tools and the different ways of stealing accounts, credit cards' number and users' confidential information, unfortunately, these thefts led to many problems and risks. The statistical analysis shows more than 3.5 million victim of hacking each year in the United states, alone. Website authentication is an important thing to protect the important information for internet users who use a web server to reach/access the information and the sources; it also offers a secure background, which could be trusted while dealing with these sites. Authentication is the first step of protecting data. The objective of this project is to develop a security system which integrates some face detection algorithms that rely on many common classification algorithms combined with fleet password typing to confirm users' legality (authentication) access to websites and related services for the purpose of increasing the security levels of special websites, moneychanger machines and other services which are offered and protected by websites. Recognizing security penetrators by feature extraction took the first place because of the numerical gabs. The password-typing fleetness would has an extensive effect on authenticating amelioration and reduce the unfavorable negatives. By applying this integration, I am seeking to reach future results that provide more assurances about the user if he/she is a penetrator or not in order to generalize his/her photo on the specialized security centers.

Keywords: *Face detection, Feature extraction, Classification Algorithms, Website Authentication.*

1. INTRODUCTION

Websites securing is a real security trepidation for researchers and websites owners due to the development of hacking tools. The majority of researchers considered that the authentication in logging in to any site is the first essential step to protect websites and its linked services. Many algorithms have been suggested to verify users. Those algorithms led to develop the authenticating man as the following:

- The differentiating between human beings and the machine CAPTCHA
- Security questions.
- Consistency due to recovery mail.

- Consistency due to mobile number.
- The development of guessing the

Security questions algorithms in addition to incompetency of depending on emails in the authenticating manners still have weakness point

That are imposed by shiftiest to access sites. Face recognition techniques is the most important new manner that are used in the clarification process to protect the important sites. Face Recognition consists of three main steps:

First, detecting and recognizing the user's face through the camera: most of the researches depended on PCA algorithm. It is one famous manner of choosing features and decreasing the dimensions. It

is called (eigneface). It selects a distinctive space that decreases distance of the general data. Then this decreased space is used in the distinction process. However, the weakness of the distinction strength inside the lyre and the large calculation are the common problems of PCA algorithm.

Second, feature extraction: the target of this stage is representing the user's face as a ray that contains the user's distinctive face features. This ray is saved into logging in database to be used later on in the classification stage in order to achieve the consistency between the face of the user whom trying to log in with his own saved ray. Most researches concentrated on PCA algorithm in feature extraction because it merges two essential stages then detected and recognize the face. However, the weakness of the distinction strength inside the lyre and the big calculations are the common problems of this algorithm.

Third, Achieving consistency by using classifiers: In face, detecting domains, which use photo processing, classification algorithms, are trained on a radial space specified in a particular group of faces photos in order to build a model that could be depended on it later on in the face consistency of the user's photo during logging in with the saved user's ray.

In this research, we developed an authentication manner by integrating many algorithms to recognize face features perfectly. In tis section, we will put essential inputs to be used by computer to recognize if this user is the real owner of this account. Three fundamental steps do this; each one uses the best algorithm:

1. Build a recorder specialized in training 130 picture.
2. Representing the photos of this recorder radially due to three stages.
 - a) Face detecting from training photos, in this stage we used Viola-Jones algorithm.
 - b) Special features extraction for each face using Land Mark algorithm to put essential points on the face and calculate the Euclidean distance between these points.
 - c) Representing the photos in a radial space depending on the extracted features.

3. Training the classifiers on the radial space and building a recognizing model then deducting the best algorithm by comparing the famous algorithms working on the shambles. At the end, we use Forest of Random Trees algorithm.
4. Using the recognizing model in conformity process.

Finally, we will input the speed of password typing and calculate the needed time to enter the user's password and comparing it to his previous entrances. The password typing time must be in the time that the user determined it due to hid last entrances.

Our research provided higher reliable authenticating results especially after merging speed of typing the password with face detecting algorithm. The results reached 78.5% to 21.5% the percentage of the loss that comes from the image's quality that is passed to the classifier.

2. RESEARCH MOTIVATION

This research aims to develop an authenticating method by merging face detection algorithms with fast typing in order to make sure of users identity by analyzing features extraction. Depending on the security, level of the targeted website in applying photo-analyzing algorithms and revealing who is trying to penetrate hack the site to reach the data that is saved on the server [1].

The results of this research would be applied on a prototype that will analyses the features extractions according to previous steps (six steps).when the entering of the name (user's name and password)fails for the first time, algorithm will compare the expeditiousness in database , if the speed wasn't close to the saved value , the second algorithm will automatically start . This classification algorithm is a recognition of features extraction.

In addition, comparing the reached results with the saved data within the database using data mining algorithms [2]. This prototype is supposed to be suitable to develop a proper tool that could be used in websites.

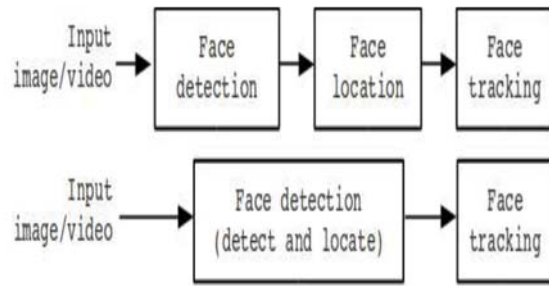
3. FACE RECOGNITION

Face recognition is considered the most associated application of photos ANALYSIS; it considered a challenge to build A TECHNICAL SYSTEM that equals the human ability of recognizing FACES. Although human being capacity of recognizing FACE, he / she is not able to recognize that while dealing with a huge amount of unknown faces. THUS, computers should overpass humankind limits by their unlimited memories and their speed of calculating and processing DATA. Face Recognition stays unpolluted task and a requested technique.(schedule 1-1) Shows the most important face Recognition applications usage with a simple research with the clause (face recognition)the results show (9422results , 1332essays in the IEEE in one year , 2009)include many examples of video monitoring, mechanical communicating, camera photos , virtual reality , where face recognition is a concept of recognition types , nerve web , computer chartings , photo processing , psychology. Engineering had got interested in face recognition in 1960. The first research was Woodrow W.BLEDSOE; He started his RESEARCH, LIKE the other researchers, by a limited panoramic RESEARCH [3] [4] [5] [6]. His most important work was Palo ALTO, California.

A. Face Detection

Face detection theories share general steps:

First, some data dimensions are decreased to achieve a response in an acceptable time. Some previous processes could be done before that to reach photo data in the preconditions of the THEORY. Then , the theories analyses the photo as it is and other theories try to extract the united and limited face extractions> the next process usually contains extracting face features or the standards in which they will be weighted , evaluated , measured or compared later on to decide if there is a face and where is it ..FINALLY. Some theories have an instructional routine contains new data for their models.

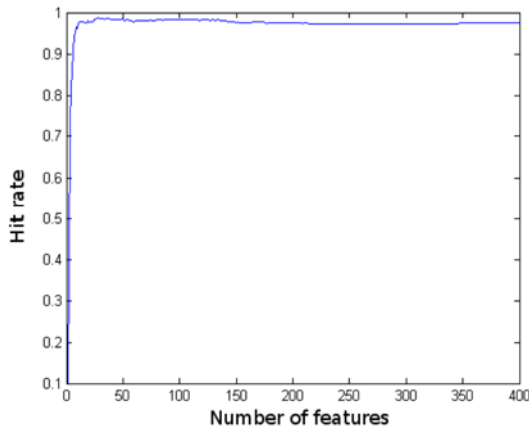


(Figure 1 : scheme box of recognizing the taken face taken from [7])

Then, face recognition is a double bind task that we should decide if there is a face or NOT. This method could be a simple task to recognize the face, it should classify the given face .technically, there are many filtered faces, and as a result, many ways to detect the face. The used techniques in face detecting is the same that used in face recognition.

B. Feature Extraction

Anyone can recognize faces from the age of five; this process seems to be an automatic exploratory process in our minds. This matter is widely ARGUMENTATIVE; OBVIOUSLY, we can recognize people we know even when they put on sunglasses or hats. We also can recognize bearded men or our grandmother in her wedding dress even though she was 23 years old in the photo. This process seems to be easy and simple but it is a challenge for computers. In FACT, the real problem is to deduct information from a photo's data. The result of this detecting must be a value with an acceptable incorrect average .the next step of face detection must be a sufficient feature detecting in the given time and the used MEMORY. The data must be better for the classification step.



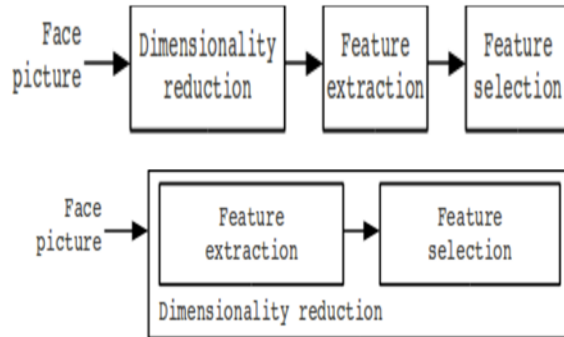
(Figure 2: PCA algorithm taken from [7])

Feature detecting contains several STEPS:

Reducing the dimension is considered as the basic mission in any determination pattern system. The classification performance depends on photos number in the SAMPLE, the number of its features and the classifications complexity. One would think that the average of the positive erroneous results of the classification does not increase like the increased features. The added features could decrease the performance of the classification theory (model 3-1). This could occurs when the number of training samples is less than the number of the features. This is called Curse of Dimensionality or Peaking phenomenon this proper method to avoid this phenomenon is by applying it at least ten times for both training samples and the number of the features, this should be enough when constructing the classification. The mentioned measurement increase by the complexity of the CLASSIFICATION, THIS curse is considered as one cause of the importance of remaining the lowest number of features. The second cause is the speed in which the classifier would be faster and use less MEMORY. At the END, the number of the features must be accurately CHOSEN, and if less or more number of features was FOUND, it will lead to loss accuracy in the recognition system. We can separate between feature deducting and feature CHOOSING. The two ways are used alternately although, we must separate between them. The process of feature detecting determines the features from data. This new features are created depending on merging the basic data , in other words , features detection changes and blends data in order

to choose the proper minor spatial from the feature's main spatial.

Feature extraction chooses the best minor assembly among the inputted feature assemblies and clarifies the unconnected FEATURES. Choosing the feature usually done before detecting the features from the face photos.



(Figure 3: scheme box, face recognition taken from [7])

Many feature extraction theories would be discussed later on in this RESEARCH. Many of these theories were used from other areas. Researchers used many methods and theories to achieve their purpose. In 1901, PCA was INVENTED, and then Karl Pearson applied it in face detection in 1995, the index below shows some of feature extraction methods to detecting faces.

(Table 1: the most important face recognition algorithms)

Method	Notes
Principal Component Analysis (PCA)	Eigenvector-based, linear map
Kernel PCA	Eigenvector-based , non-linear map, kernel methods uses
Weighted PCA	PCA using weighted coefficients
Linear Discriminant Analysis (LDA)	Eigenvector-based, supervised linear map
Kernel LDA	LDA-based, uses kernel methods
Semi-supervised Discriminant Analysis (SDA)	Semi-supervised adaptation of LDA
Independent Component Analysis (ICA)	Linear map, separates non-Gaussian distributed features

Neural Network based methods	Diverse neural networks using PCA, etc.
Multidimensional Scaling (MDS)	Nonlinear map, sample size limited, noise sensitive.
Self-organizing map (SOM)	Nonlinear, based on a grid of neurons in the feature space
Active Shape Models (ASM)	Statistical method, searches boundaries
Active Appearance Models (AAM)	Evolution of ASM, uses shape and texture
Gabor wavelet transforms	Biologically motivated, linear filter
Discrete Cosine Transform (DCT)	Linear function, Fourier-related transform, usually used 2D-DCT

C. Classification Algorithms:

There are three concepts that are considered as classifier's constructing keys (resemblance – possibility – decision dimension):

1) Resemblance:

This approach use a simple conjectural METHOD, the similar patterns should assign the similarity and represents the same category. In other WORDS, A certain matrix should be Euclidean DESIGNED, the represent age of the category could be a ray and the matrix could take an affirmation base WITH (1-NN) for every pattern within this CATEGORY. &&&&&. This approach is equivalent to the non-subjective learning, other methods could be used, like (Victor Quantization, learning Vector Quantization, self-organizing – maps – means clustering). Templates matching is another example of this approach, which is made to find out a face deduction (SCHEME BOX, the most famous Resemblance classification algorithm).

(Table 2: the most important resemblance algorithms)

Method	Notes
Template matching	Assign sample to most similar template. Templates must be normalized.
Nearest Mean	Assign pattern to nearest class mean.
Subspace Method	Assign pattern to nearest class subspace.
1-NN	Assign pattern to nearest pattern's class
k-NN	Like 1-NN, but assign to the majority Of k nearest patterns.
(Learning) Vector Quantization methods	Assign pattern to nearest centroid. There are Various learning methods.
Self-Organizing Maps (SOM)	Assign pattern to nearest node, then update nodes pulling them closer to input pattern

2) Possibility

Some applications are made depending on the possibility APPROACH. The Bayes could be renewed taking in consideration many features related to another database that may cause losing CLASSIFICATION. The presumptive database can give a definite CLASSIFICATION. The wrong presumption may be the best standard to evaluate FEATURES, thus the uncompleted potential functions could be definite.

(Table 3: the most important possibility algorithms)

Method	Notes
Bayesian	Assign pattern to the class with the highest estimated posterior probability
Logistic Classifier	Predicts probability using logistic curve method
Parcen Classifier	Bayesian classifier with Parcen density estimates

3) **Decision dimension:**

This approach could be equal to the presumptive THEORY, IT depends on the detailed matrix .The main idea is decreasing (false MEASURING) standard among filter's base and the test BASE. Fisher's linear Discriminant is one example that usually uses LDA and FLD MUTUALLY; it is close to PCA TRANSFORMERS. FID is used in an attempt to symbolize the difference between data CATEGORIES.

It could be used to decrease the basic error /FAULT; other theories use the multilayer perceptron that permits the non-linear decision DIMENSION.

The Multilayer perceptron can training differently and lead to diverse classifications that reveals CLASSIFICATIONS COMPETENCY that offers closers to the following POSSIBILITIES. The classifier could make benefit of the three concepts of classification and confirming the usage of the Euclidean distance standard.

Decision tree is trained by the repetition of single feature choosing that are more obvious in every tree NODULE. During the classification, we only need the needed features to compose the chosen feature implicitly then the decision dimension are repeatedly composed .The data (7) SHOWS some Decision trees.

(Table 4: Decision algorithms)

Method	Notes
Fisher Linear Discriminant (FLD)	Linear classifier. Can use MSE optimization
Binary Decision Tree	Nodes are features. Can use FLD. Could Need pruning.
Perceptron	Iterative optimization of a classifier (e.g. FLD)
Multi-layer Perceptron	Two or more layers. Uses sigmoid transfer functions.
Radial Basis Network	Optimization of a Multi-layer perceptron. One Layer at least uses Gaussian transfer functions.
Support Vector Machines	Maximizes margin between two classes.

4. **WEBSITE AUTHENTICATION**

The current websites use many ways to authenticate user's accounts, avoid larceny, give them privacy and security.

A. **Differentiating between the machine and human being CAPTCHA:**

In this manner, the users is given special words in a particular domain or without specifying in a zigzag way or an upper slant font to guess and retype the given words in its special place , thus we could be assure of human ability of interpenetration of the account. This security /protecting method is not certain and it can comprehend its data then submit it to the sit regarding that the user understood what is written [8].

B. **SECURITY QUESTIONS :**

In this manner, the user is given a set of questions from a list during logging in and he /she chooses one of these questions to answer in order to confirm logging in. this manner , like the previous one , doesn't offers enough security . If ONE OF the user's friends knows him WELL, he would be able to guess the answer of the SECURITY [9].

C. **RECOVERY MAIL :**

In this method, we provide them the other option of sending the mail to another account of ours/our belongings/our friends so that the passwords/links will be sent to their mails and to some extent the hacking may be avoided. By this also there is A drawback that if account is deleted then we may not provide secure [8].

D. **MOBILE NUMBER :**

This manner asks the user to type his mobile number to send him passing numbers via a SMS, thus nobody will be able to see passwords expect the user, in this case, the problem could appear when the mobile number is lost or the mobile itself was hacked [8].

E. **GUESSING THE PHOTOS IN OUR ACCOUNT :**

The user will be given a CHOICE TO GUESS a photo that exists in the user's account, but the

problem would be that the user's friends are with him in the same account, they will know the entire user's photos, they would be able to login the account, and this will be unsecured [9].

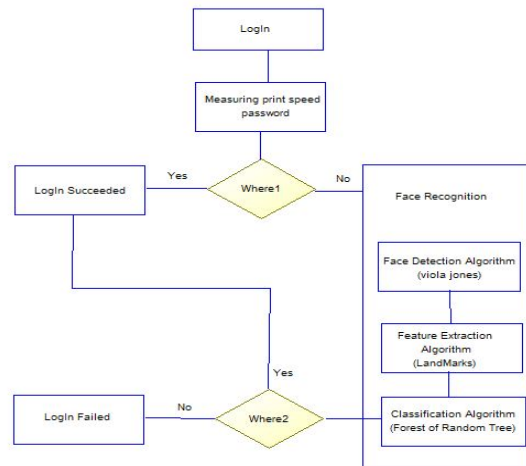
F. IMAGES AT TIME OF REGISTRATION:

The user should register in one specific PHOTO, this photo must be given at the time of REGISTRATION, AND THE problem here is that the user should take the same photo with him to every place he GOES [1].

Tacking these problems in CONSIDERATION, I suppose a new manner to protect account by merging between password typing speed and face recognition.

5. RESEARCH INFRASTRUCTURE

The objective OF this project is to develop a security system which integrates some face detection algorithms that rely on many famous classification algorithms combined with fleet PASSWORD TYPING to confirm users' legality (AUTHENTICATION) access to website and related services in purpose of increasing the security levels of special websites, moneychanger machines and other services which are offered and protected by websites. Recognizing security penetrators by feature extraction took the first place because of the numerical GABS. The password typing fleetness would has an extensive effect on authenticating amelioration and reduce the unfavorable negatives. By Applying this INTEGRATION, I am seeking to reach future results that provide MORE ASSURANCES ABOUT the user if he/she is a penetrator or not in order to generalize his/her photo on the specialized security centers.



(Figure 4: Flow chart of the system)

A. Face Detection:

It is one of the PCA's algorithms, which is known as kahuna love APPROACH. It is one of the most famous ways of features choosing and dimension decreasing. It is KNOWN, AS be Turk [10] and Puntland Eigen face. A certain distance is selected to decrease the original data' distance. Then these decreased data would be used in the detection. The weakness of the distinguish strength within the layer and the big calculations are common problems in PCA .Pol Viola and Michael Jones made a revolution in computer's DOMAIN, FACE detection by USING THE computer. After years of RESEARCHING, THEY conformed an algorithm that detect accurate photos IMMEDIATELY. This algorithm is CALLED (Viola – JONES) [11], it is CONSIDERED A simple and quick algorithm that is used in many CAMERAS. Viola and jones ignored the task of the huge DIMENSION, their trick was to concentrate on Recognition and face detection from the front/ brow ignoring looking at it from the other SIDES. Using this dimensions determines that the nose from a vertical line that rises more than eye's cavity near the NOSE. They also noticed that eyes are usually sets in shadow and from a dim horizontal BOUND. That is why they composed an algorithm that firstly, searches on a raised vertical bound in the photo that may refer to the nose then it will search for the horizontal bound that conforms the eyes. After that, it will search for other general features. These indexes are revealed one by in a series that

considered as a strong index of facial existence in the photo due to the simplicity of applying these TESTS; this algorithm can process quickly in the real TIME. Viola-Jones Algorithm can strict the real time process in the face detection servers because that it works just on the faces that are shown from front /fore head and not from other visual angle .By applying Viola –Jones ALGORITHM, data it's speed we had results that are 78.5% better than those from PCA algorithm that recorded 70% on a set of photos and 130 photos.

B. Face Extraction:

Most of research algorithms concentrate on PCA algorithm because it merges two essential stages then recognizing the FACE. However, the weakness of recognition strength with in the layer and the huge calculation are the common tasks in this faced algorithm. In this RESEARCH, WE GET to a research that dealt with facial landmark algorithm .Pedro tome reached results better than PCA's results. It depended on FIGURING OUT essential points in the face then calculating the Euclidean distance between each point and the other to get a ray that distinguish among faces then these rays are sent to the CLASSIFIERS. The first step of this algorithm is passing the photo that CONTAINS THE FACE, this process is an algorithm output as the following PHOTO:






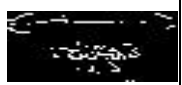




(Figure 5: input photo algorithm)

In the next STAGE, the photo will be cut into two half then the eyes and mouth will be selected in dependent photos to them transform them into bordered photos as the following ONES:

(Table 5: cutting the photo and transform it into bordered one)

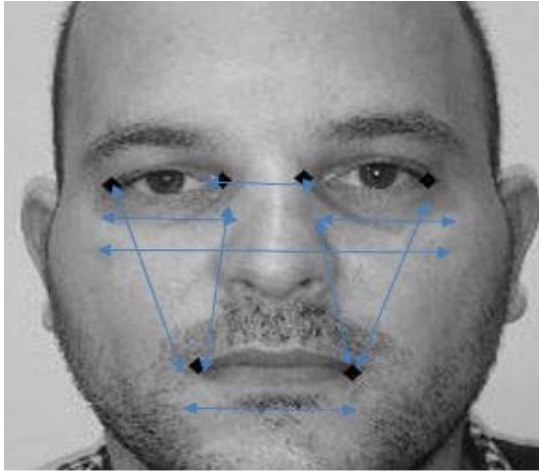
After that photo will be passed into a ring to reveal a white pixel and lean this point's coordinates as the FOLLOWING:

				←	
TRANSFORMING EYES PHOTOS INTO BORDERED ONE AFTER CUTTING THESE					THE UPPER PART OF THE FACE
				←	
TRANSFORMING OF THE BORDERED MOUTH PHOTO					THE NETHER PART OF THE FACE



(Figure 6: the final algorithms output)

In the last STEP, the Euclidian dimension would be calculated after getting the essential point of the FACE.



(Figure 7: the dimension of the face)

FINALLY, the results will be ray that distinguish every face from the OTHER. These rays will be passed to the classifier as the next scheme SHOWS:

(Table 6: Algorithms results)

description	distance
Left Eye Width	41.05
Right Eye Width	46.01
Mouth Width	57.08
Distance Small Between Eyes	30.02
Distance Large Eyes	117.02
Distance Large Between Left Eye and Mouth Left Corner	83.38
Distance Small Between Left Eye and Mouth Left Corner	79.51
Distance Large Between Right Eye and Mouth Right Corner	86.65
Distance Small Between Right Eye and Mouth Right Corner	84.93

C. CLASSIFICATION:

Most of the researchers depend on the pre-processed face photo and the inputted features that are entered into the classifiers IMMEDIATELY. However, a research the classification was divided into three main parts started with photo processing and figuring out the face within IT. The outputs of this stage are the inputs of the classification process when researchers have the following results the results of the previous [12] RESEARCHES:

(Table 7: the results of the previous researches of classification algorithms)

Classifier Name	TP Rate	FP Rate	Precision	Recall	F-Measure	ROC Area
Bayes Net	0.716	0.093	0.764	0.716	0.735	0.886
Naïve Bayes	0.541	0.189	0.564	0.541	0.549	0.76
K Star	0.508	0.263	0.49	0.508	0.496	0.696
Classification via Clustering	0.363	0.37	0.321	0.363	0.337	0.497
Filtered Classifier	0.868	0.079	0.878	0.868	0.869	0.952
END	0.865	0.083	0.872	0.865	0.864	0.957
JRIP	0.858	0.089	0.865	0.858	0.857	0.894
Ridor	0.842	0.083	0.839	0.842	0.839	0.879
Decision Table	0.871	0.078	0.883	0.871	0.872	0.955
J48	0.861	0.086	0.862	0.861	0.859	0.88
Simple Cart	0.482	0.482	0.232	0.482	0.313	0.483

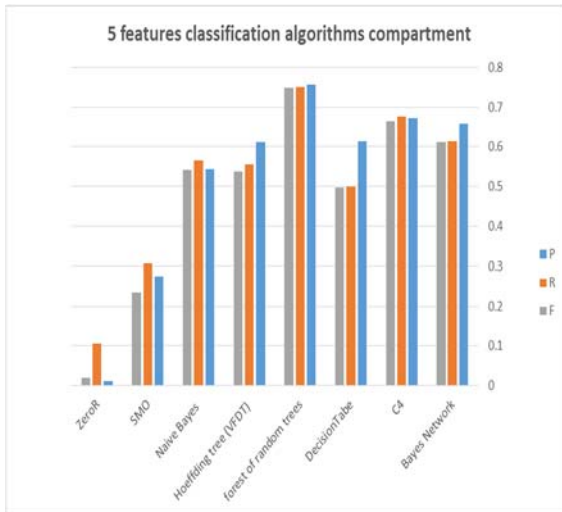
6. EXPERIMENTAL RESULTS

At the beginning of the PROJECT, we trained 5rays for every PHOTO, the features of the first training model ARE:

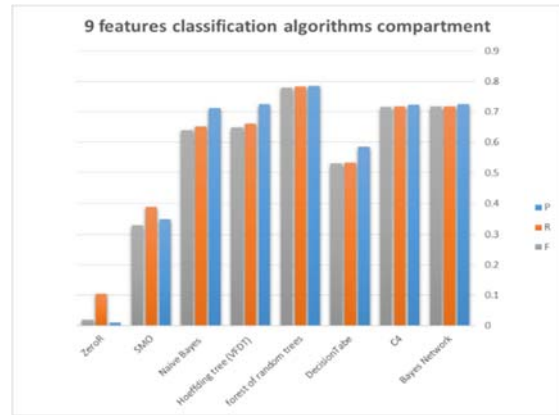
- Left Eye width
- RIGHT Eye width
- Distance between the external point of the right eye and external point of the left eye
- Distance between the internal point of the right eye and the internal point of the left eye
- Mouth width

These result revealed that the security level is weak because of feature's likeness.

However, we used this point to put several security level in the system .The forest of random trees algorithm proves the best result of classification.



(Figure 8: Five features classification algorithms compartment)



(Figure 9: Nine features classification algorithms compartment)

After THAT, nine rays was TRAINED, the features in the first raining shambles WAS:

- Distance between external right eye and mouth right corner.
- Distance between external left eye and mouth left corner
- Distance between internal right eye and mouth right corner.
- Distance between internal left eye and mouth left corner.

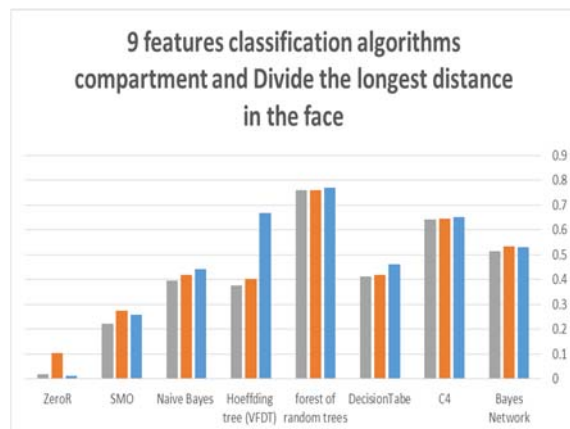
After the TRAINING, the increasing of inputs rays reveals the more ACCURATE. The following scheme shows the results of these algorithms RESULTS Figure (15) these results proved a more powerful security level because of the increasing of the features' number. Forest random trees also proved the best results Figure (15) 9-feature rays classification ALGORITHM.

Depending or random forest training RESULTS, we trained 8 famous classification algorithm that revealed the most accurate classification results depending on its RAYS. Like the scheme shows:

Algorithm	Result		
	P	R	F
Bayes Network	0.724	0.718	0.718
C4	0.723	0.718	0.715
DecisionTab	0.586	0.532	0.53
Forest of Random Trees	0.785	0.782	0.779
Hoeffding tree (VFDT)	0.724	0.661	0.649
Naive Bayes	0.712	0.653	0.64
SMO	0.35	0.387	0.329
ZeroR	0.011	0.105	0.02

(Table 8: classification algorithms training)

After that, we measured all the divided features that we have got in the longest dimension in the face photo and the results are in the next scheme:



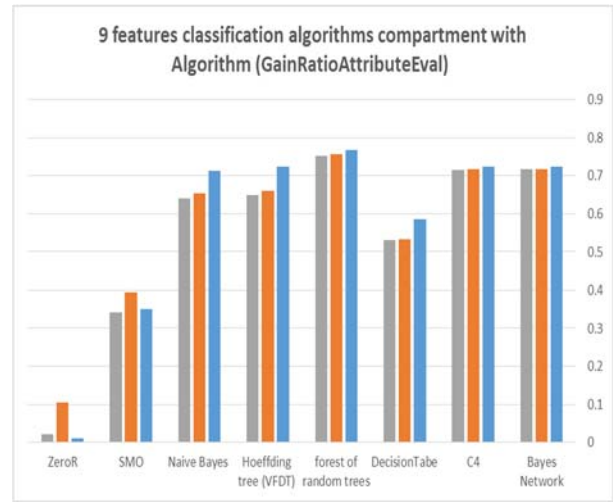
((Figure 10: nine features classification algorithms compartment and Divide the longest distance in the face)

After the training , we get the most effecting feature on the classification process which is the first feature depending in Gain Ratios algorithm that attributes Evaluate features as the following . The next scheme shows these values evaluating ON 9 features, AND the results are:

Attribute	Scores
Right Eye Width	33.064516129032 3
Left Eye Width	30.645161290322 6
Distance Large Eyes	26.612903225806 4
Distance Small Between Eyes	22.580645161290 3
Mouth Width	22.580645161290 3
Distance Small Between Right Eye and Mouth Right Corner	21.774193548387 1
Distance Large Between Right Eye and Mouth Right Corner	20.967741935483 9
Distance Small Between Left Eye and Mouth Left Corner	14.516129032258 1
Distance Large Between Left Eye and Mouth Left Corner	12.903225806451 6

(Table 10: the results of evaluating ON 9 features)

The following diagram shows the standardization of these values on the nine attributes and obtaining the results shown in the following diagram:



(Figure 10: nine features classification algorithms compartment with Algorithm (GainRatioAttributeEval))

7. FUTURE WORK

A. FACE SYMMETRY:

A face is the most common featured numeration used after THUMBPRINT. Its symmetry made it famous in several domains such as human-computer interaction HCI, legal authentication. The concept of face recognizing relies on two roles: training and testing, the training usually done without internet CONNECTION, when the accurate test is done in the real time. When database-measuring average increases, the recognizing system time increases. Human face is a vertical symmetry that is used in half's manner. Training researches revealed that half-face recognition is enough to recognize the face more than the whole symmetry. We applied the single element PCA algorithm in both manners. The accuracy was the SAME, but the average of the half-face recognition is half the average of the whole FACE [13].

B. COVERED FACES:

Many faces recognition systems were developed, some of them used in commercial productions. The face recognition process IS SENSITIVE towards face outcrop changes in photos due to lightening expressions , view, age, beards, figures ,etc.... these kinds of changes should be separated into two main categories, organized changes and unorganized ones. The organized shape's change is an expected change to cause

similar changes in the shape of different faces. The MODELLED, organized changes of shape due to LIGHTENING, DIRECTION, sharpness, and expressions changes. The unorganized change's sources come from the irregular hiding of face's part. Sunglasses and exposing the covering ORGANISMS (BEARDS, hats, AND HANDS) are considered as perfect examples of the disorganized changes [14].

8. CONCLUSION

In this RESEARCH, we proposed a developed authentication manner to recognize faces due to the best way. (IN this SECTION, WE will put essential inputs that the computer will depend on to figure out if the user IS THE real owner of the ACCOUNT). Three essential STEPS do this; each one of them used the best ALGORITHM:

- Face detection: in this step Viola - Jones algorithm is used .
- Feature EXTRACTION: LANDMARK ALGORITHM is used to put the essential points on the face and calculating the Euclidean distance between them.
- CLASSIFICATION: This is the final stage. The best algorithm is deducted by the most famous algorithms comparison on the figured samples.at the END, FOREST of Random trees algorithm is used .

After that, the password typing speed will be entered and the time of this entrance would be calculated and COMPARED WITH the previous entrance TIME. The password must be typed at the given time that the user determined due to his previous entrances.

After the merging process that we did , we reached to 78.5% better results compared with the last researches .it is expected to has a huge effect on improving user's authenticating and reduce the previous negatives.

REFERENCE

- [1] Image processing: the " P. C. Petrou .& .M .2010 "Sons & John Wiley "fundamentals
- [2] Development of " S. A. M. Caindoy .& .K. M. A a big data application architecture for Navy "Manpower, Personnel, Training, and Education Naval Postgraduate School Monterey United .2016 "States
- [3] The model method in facial " W. W. Bledsoe Palo Alto. "recognition panoramic research inc p. CA, Technical Report, Technical Report PRI .1964 "15
- [4] Man-machine facial " W. W. Bledsoe .1966 "p. 22 "Rep. PR "recognition
- [5] Some results on multicategory " W. W. Bledsoe "Journal of the ACM (JACM) "pattern recognition .1966 "pp. 13(2), 304-316
- [6] A survey of face " J. J. J. Pandya .& .J. M. R. D International Journal of "recognition approach "Engineering Research and Applications (IJERA) .2013 "pp. 3(1), 632-635
- [7] Facial " K. P. 2. F. I. C. o. (. Agrawal .& .S expression detection techniques: based on Viola and Jones algorithm and principal component & Advanced Computing "analysis February "Communication Technologies (ACCT) .2015
- [8] Security issues " R. S. R. Inukollu .& .V. N. A. S "associated with big data in cloud computing Its & International Journal of Network Security .2014 "pp. 6(3), 45 "Applications
- [9] Anti-Phishing " S. M. Kumari .& .D. A. R. K. R "Based on Face Recognition and Bio-Metric International Journal of Innovative Research and .2014 "(12)p. 3 "Development
- [10] "Eigenfaces for recognition " P. A. Turk .& .M pp. 3(1), 71- "Journal of cognitive neuroscience .1991 "86
- [11] An Analysis of the Viola-Jones " Y. Q. Wang Image Processing On "face detection algorithm .2014 "pp. 4, 128-148 "Line
- [12] M. N. Ahmeda .& .R. A. E. D. S. M. E. M. S Performance study of classification algorithms " for consumer online shopping attitudes and Communication "behavior using data mining April "Systems and Network Technologies (CSNT) .2015
- [13] Face Recognition Using "" G. C. N. A. K. Singh Indian Institute of Information "Facial Symmetry .2010 "Technology, Allahabad, India
- [14] Person identification from heavily " A. Lanitis Proceedings of the 2004 "occluded face images pp. ACM symposium on Applied computing ACM .March 2004 "(pp. 5-9)