IJRAR.ORG E-ISSN: 2348-1269, P-ISSN: 2349-5138

INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS (IJRAR) | IJRAR.ORG

An International Open Access, Peer-reviewed, Refereed Journal

SECURE DIGITAL PAYMENT TRANSACTION USING FACE RECOGNITION

Narmatha. P
Assistant Professor
Department of ECE
Excel Engineering College, Namakkal.

Ragul M, Shafeer Mohamed I, Vana bharath S, Subash S
UG Students
Department of ECE
Excel Engineering College, Namakkal.

Abstract:

The danger of exchange coordinated out or pernicious programming (malware)- based assaults or unlawful utilization of innovation is huge and developing; simultaneously web based banking gets increasingly well known. Prior, during making any web-based installment or making any web based banking related exchanges, the technique used to finish an exchange was with One-Time-Passwords as well as passwords, which were sent on the end clients enlisted versatile number or email address which were connected with his financial balance. Monetary misfortune might be one of the outcomes assuming that certifications or qualifications connected gadgets get taken. In numerous conventions, the exchange data isn't gotten as expected. The proposed "Validation of Digital Payment utilizing Face Recognition" depends on the face acknowledgment procedure on installment door. This framework wipes out the One-Time-Password and secret word based exchanges with Face acknowledgment framework. Whenever face acknowledgment verification is utilized, parodying or faking of face comes into picture. As in face acknowledgment, faking should be possible by showing photo (printed copy) or video before the confirming gadget. Considering these faking or parodying strategies, the framework additionally utilizes Face ridiculing calculations to conquer these issues. Utilizing this we can finish fruitful exchange by checked regular individual such that it is demonstrated to the executing party, that the exchange was as a matter of fact started and affirmed by a distinguished normal individual.

Keyword: Portal, Digital Payment, Payment Portal, Face recognition, Authentication.

I. INTRODUCTION

The Portal is called as Trusted Third Party or Entry point to any network. It is used in E-commerce system for more secure transaction. Online shopping allows customers to sit in their homes and buy goods from all over the world. Similarly allow Merchant to sell their products to all over the world from home. Most of the population will use online payment in near future. Most of the world's countries lagged behind in making a good Internet architecture[1]. There is need of a secure, fast and easy online payment Portal which is more reliable. On the basis of proposed architecture of Digital Payment system, this systemgives a brief overview of Digital Payment using face recognition. It also mentions the requirement of an Digital Payment Portal from customer and merchant's point of view. And on the basis of these facts and figures, a new secure Digital Payment has been designed and developed. The payment would provide secure and fast transactions. On the basis of proposed architecture of Digital Payment system and the requirements related to any electronic payment, we design and develop a secure, reliable and efficient electronic payment with face recognition. Now-a-days, in India the concept of Digital Payment is getting more popular than earlier. The networks, run by banks and the government over high-speed phone lines, converge at just 10 secret data processing centres nationwide. They transmit everything from direct-deposit pay checks to utility bill payments to huge corporate transfer in the India and abroad. On second priority speed of transactions comes. This proposed idea has a scope of developing such a system that will provide a secure, reliable and fast transaction processing using Face Recognition. In Face recognition system, when a request is generated for transaction, the details of the payee are verified. If the details are legitimate i.e. payee is legitimate, then the facial details of payee are collected and simultaneously it is collected by the corresponding bank and compared with each other. Positive response of comparison will lead to successful transaction processing. Whereas, negative response will lead to termination of the transaction. And, if the user is not legitimate then the transaction processing is rolled back to merchant's website. This working of the system will eliminate the OTP based transaction processing as well as make the payment secure, efficient and faster.

II. PRELIMINARIES

Online customer:

A customer is an entity who will buy products by makingpayments in timely manner.

Merchants:

A merchant is a seller who will receive payments made bycustomer.

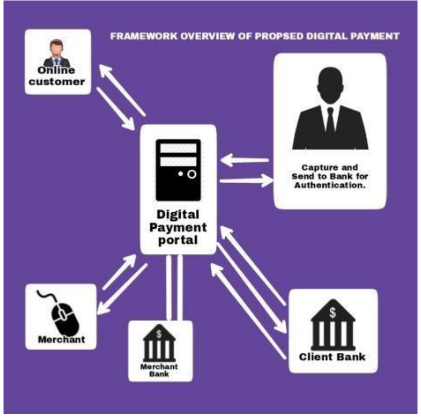

FRAMEWORK OVERVIEW OF PROPSED DIGITAL PAYMENT
Online customer
Capture and Send to Bank for Authentication.
Digital Payment portal
Merchant
Merchant Bank
Client Bank

Figure.1.Framework Overview of Proposed Digital Payment Banks:

Two banks involved are:-

1. Client bank
2. Merchant bank

Client bank:

Client's bank holds client's bank account details and validate customer during account registration.

Merchant bank:

Merchant bank holds merchant bank account details. It is responsible for management, fraud control etc. A merchant account is a type of bank account that allows businesses to accept payments by payment cards, typically debit or credit cards. A merchant account is established under an agreement between an acceptor and a merchant acquiring bank for the settlement of payment card transactions. In some cases a payment processor, independent sales organization (ISO), or merchant serviceprovider (MSP) is also a party to the merchant agreement [2].

Payment Portal:

A payment Portal is connected to all customers, merchants and banks through Internet and responsible for the speed, reliability and security of all transactions that take place. A payment Portal is an e-commerce service that authorizes payments for e-businesses and online retailers. It is the equivalent of a physical POS (point-of-sale) terminal located in most retail outlets. A merchant account provider is typically a separate company from the payment Portal. Some merchant account providers have their own payment Portals but the majority of companies use 3rd partypayment Portals.

The Portal usually has 2 components:

a) The virtual terminal that can allow for a merchant to securely login and key in credit card numbers

b) They have the website's shopping-cart connected to the Portal via an API to allow for real time processing from the merchant's website.

III. FRAMEWORK OVERVIEW

There are six interfaces:-

1. Customer Interface
2. Server (Digital Payment Portal) Interface
3. Client Bank Interface
4. Face Recognition Interface
5. Merchant Bank Interface
6. Merchant Interface

Online Customer will connect to Digital Payment Portal through Internet. Portal will connect to the Bank and check whether its bank accounts are enough to buy the required product. Online customer can also visit Merchant's website through Portal. Secure Pay provides a payment Portal that facilitates electronic commerce by enabling merchants to accept credit cards and electronic checks as methods of payment for goods and services sold online. The Portal acts as a bridge between the merchant's website and the financial institutions that process payment transactions. Payment data is collected online from the shopper and submitted to the Portal for real-time authorization. However, the payment Portal is targeted towards merchants that process Card-Not-Present transactions. In a Card-Not-Present, We proposed a model of electronic payment Portal using face recognition on the basis of facial details, such that transaction processing is done efficiently in a secure manner as fast as possible by eliminating OTP based transaction. All e- commerce and mail/telephone orders are Card-Not-Present transactions.

IV. PRELIMINARY TERM

Privacy: It is necessary to assure privacy in the payments likebank accounts.
Naming: There should be a way of identifying the customer'sbank accounts and the merchant bank accounts.
Security: In Portals security should provide to protect data oftransactions.
Integrity: Data should be difficult to change.
Confirmation: When transaction took place customer must havenotification and merchant must have confirmation
Confidentiality: Any third parties should not be able to access orview such payment.

FLOW DIAGRAM PROPOSED DIGITAL PAYMENT

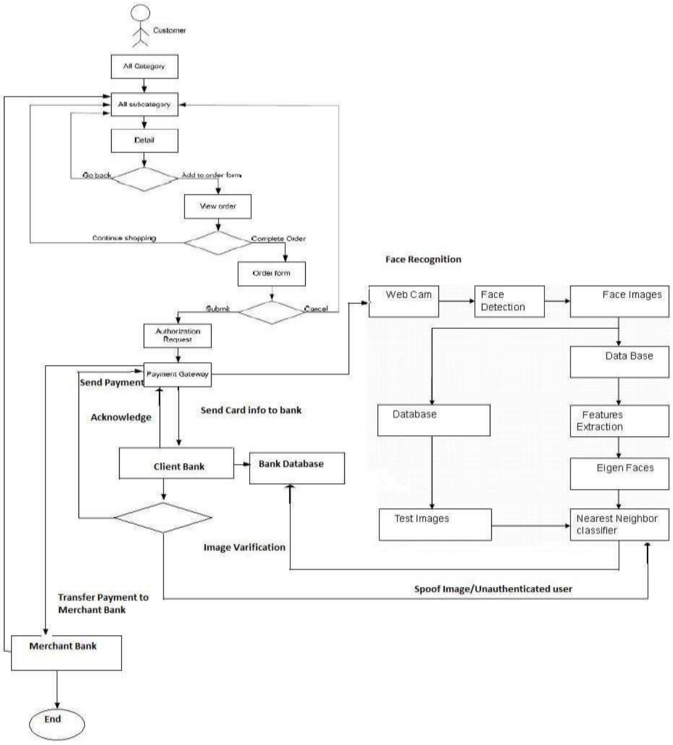


Figure.2. Flow diagram of proposed Portal

This system specially developed for encouraging Digital Payment for online shopping because of security issues. Here we use electronic Portal which is used for secure transaction between client and merchant using Face recognition by eliminating OTP based transaction. If new user wants to do transaction then he/she should register Himself/herself first through registration form then browse merchant website using Digital Payment Portal. Select item and encrypt payment request and send it to Server. Server receives encrypted message from sender, decrypt message, read, encrypt it using its own keys, encrypted facial details and send it to Client bank. Client bank first authenticates facial data which is received with the details available in database, and then the transfer of required amount is done to the merchant bank through secure network. After receiving the fund Merchant bank sends the payment.

V. TECHNIQUES & ALGORITHM

There are various algorithms on actions of client, merchant

1. Algorithm of Client:

Client can browse merchant's website. After selection of items he can send payment order to Digital Payment server after filling required fields e.g. Credit card number, expiry date etc Steps: -

1. Start and connect.
2. Start Customer browse merchant website
3. If select Category then Go to Item list of selected category
4. If Select Item ThenShow detail of selected item
5. If Want to buy selected item ThenSelect Add to order form
Else
Go back to category
6. If select add to order formDo Add To Order Sub Category Id
go to Order form and fill required fields like credit card No.,expiry Date, and telephone no, Address
7. Select SubmitElse continue shoppingElse Cancel
8. If select submit Display Authorization
9. If Credit card no. Text is equal to Credit card no. display This Customer is Authorized From Bank.

2. Payment Portal algorithmSteps: -

```
 Start connectionIf connected
   Receive payment messageElse display not connected If receive payment message
  {
     Decrypt message
     Split and send it to different textboxesAdd it to a database
     Send it to client bank
  }
 Else cancel
 If client bank is sending message
  {
     Receive it
     Send it to face recognition process
  }
 If client bank is sending message
 {
     Authorized user and payment receiverSend it to merchant bank
 }
Else wait
If merchant bank is sending message
 {
     Receive it
     Send it to merchant
 }
```

3. Algorithm of Client Bank:

Client bank receives payment message and verify client. Deduct amount from client bank and send that amount to payment Portal.**Steps: -**

1. Start connection
2. If connected
   Receive payment message including client’s information.
3. If client’s info is present in database of bank
   Send message to server This customer is Authorized
4. Else
5. Send message This customer is not Authorized
6. If customer is Authorized{Send request for Face Verification .Verify face with face present in bank Database}
7. If customer is Authorized{Save payment request into database Deduct amount from Client bank Send that amount to Payment Portal}
8. Else
9. Send message This customer is not Authorized

4. **Algorithm of Merchant Bank:** Merchant bank verifies merchant, receives payment message from Client bank through payment server and add payment to Merchant’s account.

Merchant BankSteps: -

a) Start connection
b) If connected
c) Receive payment message including merchant accountno.
d) If merchant’s account is present in database of bank
{Receive payment Add payment to Merchant’s account}
e) Else
f) Send message Invalid account no.

5. **Algorithm of Merchant:** Merchant makes and updates website and receives acknowledgement messages from payment Portal.

Merchant

Steps: -

a) Start connection
b) If connected {Make and update website}
c) If server is sending message Receive message anddecrypt it}
d) Else
e) Retry to connect

VI. FACE RECOGNITION AND SPOOFING TECHNIQUE

It has been shown that face recognition techniques are vulnerable to spoofing attacks. In a spoofing attempt, a person tries to masquerade as another person and thereby, tries to gain an access to the system. Numerous recognition approaches have been presented in face recognition topic, however the studies on face anti-spoofing methods are still very limited. Therefore, nowadays anti-spoofing is a popular topic for researchers to fill this gap. Aim is to develop non-intrusive methods without extra devices and human involvement. In this way they can be integrated into existing face recognition systems. Also, methods which are robust to pose and illumination changes are preferable.

1. Algorithm for feature extraction using PCA

The facial features are extracted using the PCA method. Let there are *R* face images in the training set and each image ***Xi*** is a 2dimensional array of size *m*× *n* of intensity values. An image ***Xi*** can be converted into a vector of *D* (*D* = *m*× *n*) pixels, where, ***Xi***
= (xi1, xi2, ….,xiD). The rows of pixels of the image are placed one after another to form the vector. Define the training set of covariance matrix is defined as follows:

$$\Gamma = \frac{1}{R}\sum_{i=1}^{R}\left(X_i - \overline{X}\right)\left(X_i - \overline{X}\right)^T$$
$$= \Phi\Phi^T$$

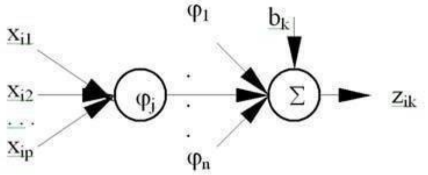
where Φ = (Φ1, Φ2, …, ΦR) ⊂ ℜ*D*×*R* and

$$\overline{X} = \frac{1}{R}\sum_{i=1}^{R} X_i$$

which is the mean image of the training set. The dimension of the covariance matrix Γ is *D*× *D* .Then, the eigen values and eigenvectors are calculated from the covariance matrix Γ. Let **Q**
= (**Q**1, **Q**2, **Q**r) ⊂ℜ*D*×*R* (*r*<*R*) be the *r* eigenvectors corresponding to *r* largest non-zero eigen values. Each of the *r* eigenvectors is called an *eigenface*. Now, each of the face images of the training set **X**i is projected into the eigenface space to obtain its corresponding eigenface-based feature Zi ⊂ ℜ*r*×*R* , which is defined as follows:

Zi = **Q**T**Y**i , i = 1, 2,…, *R* ....(2)

where **Y**i is the mean-subtracted image of **X**i.
In order to recognize the test images, each of the test images is transformed into the eigenface space using the equation (2) and then fed to the RBF neural networks as inputs for classification.



2. Algorithm for spoofing using LBPV

LBPV is a simplified and efficient joint LBP and contrast distribution method. In LBP calculation, there is no information related with variance. Actually, the variance is also related to the texture feature and usually the high frequency texture regionshave higher variances and contribute more to the discrimination of images. Since initially, DoG filtering is applied, the high frequency regions are all extracted after this step. Thereby, it is easier to discriminate captured and recaptured images byapplying LBPV algorithm on these regions which are extracted by DoG filtering. The contrast and pattern of a texture are complementary features. LBPV adds additional contrastmeasures to the pattern histogram and this provides significantly better results than LBP. This claim is verified by testing bothLBP and LBPV using different textures in . These algorithms are also tested for our study. The comparison result is given in 'Experimental Results' part of the paper. LBPV calculation is based completely on LBP calculation.
LBPP,*R* is calculated as follows:

$$LBP_{P,R} = \sum_{p=0}^{P-1} s(g_p - g_c)2^p, \qquad (1)$$

$$s(x) = \begin{cases} 1 & x \geq 0 \\ 0 & x < 0 \end{cases} \qquad (2)$$

LBPP,*R* is computed such that for a given central pixel in an image, a pattern number is computed by comparing its value with those of its neighbours. In Equation (1), gc is the gray value of the central pixel, gp is the value of its neighbours, P is the number of neighbours around a circle of radius R . To obtain LBP histogram of an X × Y image, the LBP pattern of each pixel (i, j) is used in calculation.

$$H(k) = \sum_{i=1}^{X}\sum_{j=1}^{Y} f(LBP_{P,R}(i,j),k), \quad k=[0\ K] \qquad (3)$$

$$f(x,y) = \begin{cases} 1 & x=y \\ 0 & else \end{cases} \qquad (4)$$

K is the maximal LBP pattern value in (3). In this histogram, each LBP pattern has weighting factor of 1.LBPV algorithm is used to add contrast information to this histogram. Variance is computed for the P sampling points around a circle of radius R using Eqs. (5) and (6).

$$Var_{P,R} = \frac{1}{P}\sum_{p=0}^{P-1}(g_p - u)^2 \qquad (5)$$

$$u = 1/P\sum_{p=0}^{P-1} g_p \qquad (6)$$

The LBPV computes the variance from a local region and accumulates it into the LBP bin as the weighting factors [10]. LBPV histogram is calculated using Eqs. (7) and (8).

$$LBPV_{P,R}(k) = \sum_{i=1}^{X}\sum_{j=1}^{Y} w(LBP_{P,R}(i,j),k), \quad k=[0\ K] \qquad (7)$$

$$w(LBP_{P,R}(i,j),k) = \begin{cases} \text{var}_{P,R}(i,j) & LBP_{P,R}(i,j)=k \\ 0 & else \end{cases} \qquad (8)$$

The representations of two different selections for P and R valuesare shown in Fig. 2. When P and R values are increased, even better results are obtained; however With a cost of increasing computational complexity as stated in.

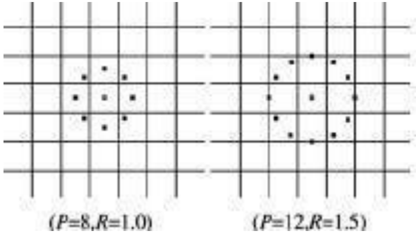


Figure.3. Circular representations of selections (P=8, R=1)and (P=12, R=1.5).

In the proposed approach, P and R values are selected as $P = 8$, $R = 1$, due to this computational complexity. Instead of using all LBPV patterns, uniform patterns can be used as features in classification part. Uniform patterns are selected according to the U value which is defined as

$$U(LBP_{P,R}) = |s(g_{p-1}-g_c)| - |s(g_0-g_c)| + \sum_{p=1}^{P-1}|s(g_p-g_c)| - |s(g_{P-1}-g_c)| \qquad (9)$$

There are both local and global rotation invariant algorithms in texture classification. In the proposed approach, a hybrid method, which is based on globally rotation invariant matching with locally variant LBPV texture features, is used to extract features for classification. Thereby, both global spatial information and local texture information are preserved in classification. In our study, this global matching is implemented using exhaustive search scheme to find the minimal distance in all candidate orientations, which is asimple method. The LBPV histogram is reorganized and represented by a rotation variant histogram *Hrv*, and a rotation invariant histogram *Hri*. Then for two texture images, the matching distance is calculated as shown in Eq (10).

$$\begin{aligned} &D_{ES}(H_S,H_M) = D_{ri}(H_S^{ri},H_M^{ri}) + D_{\min}(H_S^{rv},H_M^{rv}) \\ &|D_{ri}(H_S^{ri},H_M^{ri}) = D(H_S^{ri},H_M^{ri}) \qquad (10) \\ &D_{\min}(H_S^{rv},H_M^{rv}) = \min(D(H_S^{rv},\overline{H_M^{rv}(j)})),\ j=0,1,\ldots,7 \\ &\overline{H_M^{rv}(j)} = [h^M_{\text{mod}(0-j,8)}, h^M_{\text{mod}(1-j,8)},\ldots, h^M_{\text{mod}(7-j,8)}] \end{aligned}$$

In the proposed approach, chi-square distance is selected to beused as the dissimilarity metric, since for LBP based algorithms, it is recommended as dissimilarity metric in various studies. Chi- square distance between sample and model histograms is computed as

$$D(S,M) = \sum_{i=1}^{N}\frac{(S_i - M_i)^2}{S_i + M_i} \qquad (11)$$

N is the number of bins and Si and Mi are, respectively ,the values of the sample and model histograms at the nth bin. For each test image, matching by exhaustive search is applied using chi-square distance metric, and distances from each test sample to all samples (xi) in the client and impostor model sets are obtained. Then, quadratic means of distances arecomputed for client and impostor model sets, consecutively

.N is the number of images in the model set and xi is the distance between test sample and model sample.

VII. EXPERIMENTAL RESULTS

1. Graphical result of survey:

A survey was carried out of various users in three different areas for finding the reason that why people don't use payment Portal and wrote it by compiling tl

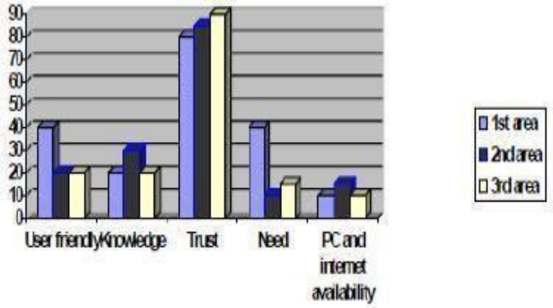


Figure.4. graphical result of survey

a. **User Friendly:** People want a payment Portal whichshould be easy to use.
b. **Knowledge:** Some people don't know anything aboutpayment Portal.
c. **Trust:** Mostly people don't use it because of lack oftrust.
d. **Need:** Some people thinks there is no need of DigitalPayment Portal.
e. **PC and Internet availability:** Limited access of PCand internet.

2. Graphical result of proposed Portal:

Graphical result of proposed Portal is following , As compareto other Digital Payment Portals our proposed system will bemore secure and do transactions in less time as compare to other Portal. Proposed system will be inexpensive ascompare to existing systems.

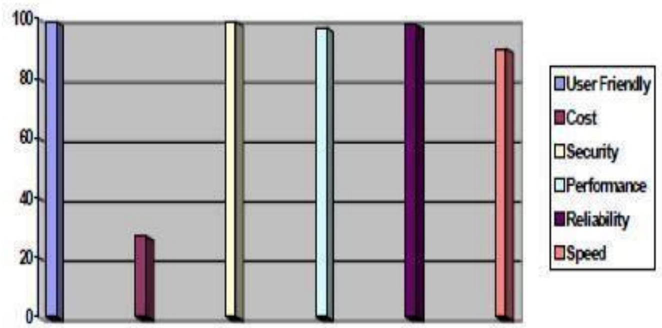


Figure.5. Graphical Result of Proposed Portal

a. **Time**: Time of transaction
b. **Cost**: E-Portal's charges per transaction
c. **Availability**: The degree to which e-Portal is operable
d. **Security**: Overall security related to electronic Portal

VIII. FUTURE SCOPE

As the Internet continues to grow and develop in the coming years, new services and technologies will also emerge. Information Systems instructors and students need not only to understand the current online payment options and their implementation, but also upcoming trends. Thus far, thistutorial focused on the e-credit payment methods currently available. Yet, other types of systems that may become more prevalent in the future such as e-cash or micropayments or options not even envisioned.

IX. LIMITATIONS

Computer cannot replace human judgment & Decision making.

For transaction through Digital Payment Portal, usermust have account in the bank which is registered on Digital Payment Portal.

The Availability of Portal must be high to be used by online customers.

Cost factor must be minimum so it can be affordedby customers.

X. CONCLUSION

The proposed Payment Portal is made secure by the execution of secure e-exchange utilizing face acknowledgment. Due to this main genuine clients can do exchanges. This installment Portal is created secure sufficient that any approved client can undoubtedly trust on it and boldly or with certainty make installments over the Internet. At first it's checked on the off chance that the client is approved one or not then the entire exchange happens. E-installment Portals satisfy all necessities and give security, protection and so on. Based on these necessities and the nearby framework, we carried out an electronic installment involving face acknowledgment for neighborhood climate.

XI. REFERENCES

[1].V. Athitsos, M. J. Swain, and C. Frankel, "Distinguishing Photographs and Graphics on the World Wide Web", in IEEE Workshop on Content-Based Access of Image and Video Libraries, pp. 10-17, June 1997.

[2]. J. Friedman, T. Hastie, and R. Tibshirani, "Additive Logistic Regression: A Statistical View of Boosting", Technical Report, Stanford University, 1998.

[3]. M. Stricker, and M. Orengo, "Similarity of color images", in Proceedings of SPIE Storage and Retrieval for image and Video Databases Conference, pp. 381-392, 199

[4]. Belhumeur P. N., Hespanha J. P., and Kriegman D. J.1997,“Eigenfaces versus fisher faces: recognition using class specific linear projection”, IEEE Trans. Pattern Anal. Mach. Intell., vol. 23, no. 7,pp. 711-720.

[5]. Chellapa R., Wilson C., Sirohey S. 1995, “Human and machine recognition of faces: a survey”, Proc. of the IEEE, vol. 83, no. 5, pp. 705-741.

[6]. Er M. J., Wu S., Lu J. and Toh H. L. 2002, “Face recognition with radial basis function (RBF) neural networks”, IEEE Trans. Neural Networks, vol. 13, no. 3, pp. 697-710.

[7]. T. T. Ng, S. F. Chang, and J. Hsu, "Physics-Motivated Features for Distinguishing Photographic Images and Computer Graphics", in proceedings of ACM conference on Multimedia, pp. 239-248, Singapore,2005.