ENHANCING USER AUTHENTICATION OF ONLINE CREDIT CARD PAYMENT USING FACE IMAGE COMPARISON WITH MPEG7-EDGE HISTOGRAM DESCRIPTOR

Mr. Gittipat Jetsiktat

A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Science Program in
Computer Science and Information Technology
Department of Mathematics and Computer Science
Faculty of Science
Chulalongkorn University
Academic Year 2014

การเพิ่มสมรรถนะการพิสูจน์ตัวจริงผู้ใช้ของการจ่ายผ่านบัตรเครดิตออนไลน์โดยใช้การเปรียบเทียบภาพหน้าด้วยตัวอธิบายฮิสโทแกรมของเส้นขอบเอ็มเพ็กเจ็ด

นายกิตติภัทร เจตสิกทัต

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิทยาการคอมพิวเตอร์และเทคโนโลยีสารสนเทศ
ภาควิชาคณิตศาสตร์และวิทยาการคอมพิวเตอร์
คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2557

Thesis Title	ENHANCING USER AUTHENTICATION OF ONLINE CREDIT CARD PAYMENT USING FACE IMAGE COMPARISON WITH MPEG7-EDGE HISTOGRAM DESCRIPTOR
By	Mr. Gittipat Jetsiktat
Field of Study	Computer Science and Information Technology
Thesis Advisor	Assistant Professor Suphakant Phimoltares, Ph.D.

Accepted by the Faculty of Science, Chulalongkorn University in Partial Fulfillment of the Requirements for the Master's Degree

.....Dean of the Faculty of Science

(Professor Supot Hannongbua, Dr.rer.nat.)

THESIS COMMITTEE

.....Chairman

(Professor Chidchanok Lursinsap, Ph.D.)

.....Thesis Advisor

(Assistant Professor Suphakant Phimoltares, Ph.D.)

.....External Examiner

(Assistant Professor Sathit Nakkrasae, Ph.D.)

กิตติภัทร เจตสิกทัต :

การเพิ่มสมรรถนะการพิสูจน์ตัวจริงผู้ใช้ของการจ่ายผ่านบัตรเครดิตออนไลน์โดยใช้การเปรียบเทียบภาพหน้าด้วยตัวอธิบายฮิสโทแกรมของเส้นขอบเอ็มเพ็กเจ็ด (ENHANCING USER AUTHENTICATION OF ONLINE CREDIT CARD PAYMENT USING FACE IMAGE COMPARISON WITH MPEG7-EDGE HISTOGRAM DESCRIPTOR)

อ.ที่ปรึกษาวิทยานิพนธ์หลัก: ผศ. ดร. ศุภกานต์ พิมลธเรศ , 81 หน้า.

ในทศวรรษที่ผ่านมาความก้าวหน้าทางเทคโนโลยีบนอินเทอร์เน็ตและเทคโนโลยีสารสนเทศได้สนับสนุนการกิจกรรมส่วนใหญ่ทั้งด้านสาธารณะและส่วนบุคคล การทำธุรกรรมออนไลน์เป็นหนึ่งในกิจกรรมที่แสดงบทบาทสำคัญในการใช้ชีวิตของผู้คน อีกทั้งยังเป็นทางเลือกเพื่อเพิ่มความสะดวกสบายด้วย อย่างไรก็ตามข้อมูลของผู้ใช้งานสามารถรั่วไหลได้อย่างง่ายดายหากไม่มีการป้องกันอย่างรัดกุม การทวนสอบโดยไบโอเมตริกสามารถนำมาใช้เพื่อแก้ปัญหาการรักษาความมั่นคงนี้ได้ วิทยานิพนธ์ฉบับนี้ได้เลือกใช้หน้าเป็นอินพุตสำหรับการทวนสอบไบโอเมตริกในกระบวนการจ่ายออนไลน์ ตัวอธิบายฮิสโทแกรมของเส้นขอบเอ็มเพ็กเจ็ดได้นำมาใช้ในการสกัดลักษณะเด่นของภาพหน้า สำหรับผลการทดลองแสดงให้เห็นว่าตัวอธิบายฮิสโทแกรมของเส้นขอบเอ็มเพ็กเจ็ดให้ผลดีกว่าตัวอธิบายอื่นๆ ดังนั้นตัวอธิบายนี้จึงสามารถนำมาใช้กับกระบวนการทวนสอบใหม่ของระบบการจ่ายออนไลน์โดยได้ออกแบบและสร้างกระบวนการซึ่งไม่ซับซ้อนยุ่งยากและมีสมรรถนะสูง ผลการทดลองบนพื้นฐานของการวิเคราะห์ผลทางสถิติได้แสดงให้เห็นว่ากระบวนการที่มีการทวนสอบการเทียบหน้าเป็นส่วนประกอบสามารถเพิ่มความมั่นคงให้กับระบบอีกทั้งเพิ่มความสามารถในการใช้งาน ประสิทธิภาพ และความพึงพอใจของผู้ใช้ได้ด้วย

ภาควิชา	คณิตศาสตร์และวิทยาการคอมพิวเตอร์	ลายมือชื่อนิสิต .....
		ลายมือชื่อ อ.ที่ปรึกษาหลัก .....
สาขาวิชา	วิทยาการคอมพิวเตอร์และเทคโนโลยีสารสนเทศ	
ปีการศึกษา	2557	

5672601023 : MAJOR COMPUTER SCIENCE AND INFORMATION TECHNOLOGY

KEYWORDS: ONLINE PAYMENT; SECURITY; TRANSACTION; CREDIT CARD; FACE MATCHING VERIFICATION; SIMULATION; PERFORMANCE EVALUATION

GITTIPAT JETSIKTAT: ENHANCING USER AUTHENTICATION OF ONLINE CREDIT CARD PAYMENT USING FACE IMAGE COMPARISON WITH MPEG7-EDGE HISTOGRAM DESCRIPTOR. ADVISOR: ASST. PROF. SUPHAKANT PHIMOLTARES, Ph.D., 81 pp.

In the past decade, progressions of internet and information technology support most of public and individual activities. Online payment transaction is one of those activities which also play an important role in people life. It is an alternative option for persons to choose for convenience. However, user information can leak easily without strictly protection. Biometric verification was considered as a key to overcome this security problem. In this thesis, face was selected as an input for biometric verification in online payment process. MPEG7-Edge Histogram Descriptor was proposed to be used in the feature extraction of face image. For the experimental results, this descriptor outperformed the other descriptors. Therefore, it can be applied to the new verification process of online payment system. Then, uncomplicated process with high performance was designed and created. The experimental results based on statistical analysis showed that the process with face matching verification can increase system security as well as improve the usability, capability, and user satisfaction.

Department:	Mathematics and Computer Science	Student's Signature .....
		Advisor's Signature .....
Field of Study:	Computer Science and Information Technology	
Academic Year:	2014	

ACKNOWLEDGEMENTS

I would like to thank all those persons who help and provide me all great support during my research.

First and foremost, I would like to thank my advisors, Assistant Professor Dr. Suphakant Phimoltares. I would have deeply lost in the research without his guidance. His immense encouragement and comments really help me understanding and pass through all journey in completion of research. I also sincerely thank, Assistant Professor Sasipa Panthuwadeethorn for her evaluable advices and her patient proofreading towards the completion of this research.

I would also like to thank Mr.Nattakan Praprutdee, Mr.Niphon Sinsawad, Miss Supaporn Arpacharudkul and Miss Jutamas Limsirinawa for their helpful suggestion and corrections on the questionnaire. Their ideas are very useful and helpful for this research and All participants for devoted their time to participating in this research.

Last but not least, I would like to give credit to my family and friends who always are by my side and give their immense support.

CONTENTS

Page

Page

Page

Content of Tables

Content of Figures

Chapter 1. Introduction

The online banking on the internet is interested to use as a channel to communicate with the bank. The widespread use online banking on the internet needs to access online data in varies types and levels. Therefore, main process to access online data is verification process which is proposed to certify the security of the online banking systems. Although password, Personal Identification Number (PIN) and signature verification are standardized procedure in verification systems, they are still vulnerable. Currently, biometric verification is a procedure that is more reliable than traditional procedure. Biometric identifiers are more unique and individual for verification. There are many types of biometrics such as fingerprint, palm prints, hand geometry, face or even iris. Among these types of biometric, one of biometrics that is the most popular to use for verification process is face. Face image was frequently used by reason of its usability, acceptability and collectability [1].

Basically, biometric verification procedure using face image consists of two steps, face detection as a pre-processing step and face verification as a main step. In pre-processing step with face detection, image of face is detected. In this step, an image is collected and stored in database. Next step is the main part for verification. In this step a person is verified from a digital image or a video containing face. The system detects a face in the image and verifies by finding out the similarity with face image in database that was stored in pre-processing step. The face verification uses image of face as a significant characteristic. Furthermore, face image can be used in behavior verification. In the face image verification, image of face acts as the most significant role to compute the similarity of face image from given database based on image content. The simple contents of image are low-level features of image (e.g. colors, texture, spatial, layout, shapes, etc.) corresponding the properties extracted from images. To

compare two images, the features are extracted from two images then a distance between two images is computed from their features to measure similarity of images [2].

From mentioned benefit of face image, image similarity is a core concept for authentication process. The face image that is kept in database can be used as significant part for the authentication process based on face verification in online banking transaction. This research aims to enhance the security system based on the chosen image descriptor, namely the Moving Picture Experts Group 7-Edge Histogram Descriptor (MPEG7-EHD). This descriptor was used to develop the proposed process of the payment system. A new authentication process with face matching verification was applied into the proposed process. The proposed process of the payment system was tested by 35 persons sample group. User satisfaction feedbacks were gathered by a set of questionnaire and in-depth interview. The feedback data were analyzed by statistical tests and analytical results were concluded as the result of this research.

1.1. Objective

In order to achieve the entire goal, three objectives were set.

1. To ensure that MPEG7_EHD works well in the authentication process, MPEG7-EHD was compared with reliable descriptors which are generally used in the face similarity method under the different resolutions of two images.
2. To enhance the authentication method of online transactions by proposing a proposed process of the payment system that uses MPEG7-EHD in face image comparison method.
3. To evaluate performance of the proposed system comparing with the traditional approach.

1.2. Scope of thesis and constraints

1. Enhanced security proposed process in online transaction based on face authentication method including the authentication on Electronic Draft Caption (EDC) transaction and the authentication on the Internet banking.
2. The proposed process was developed by Visual Basic (VB.NET) language.
3. Face images from 35 persons were used in the proposed process of this research.
4. The proposed process was evaluated by satisfaction analysis and in-depth interview.
5. The proposed process used images of size 180x180 pixels with 72 dpi. These source images were captured by web-camera in which the resolution was 0.3 mega pixels.

1.3. Expected Outcome

1. MPEG7-EHD was selected as the best descriptor in terms of reliability and compatibility for comparison between a face image captured by user's camera and the other low-resolution face image.
2. The proposed process of the online transactions with face authentication method.
3. The uncomplicated proposed process with high performance.

Chapter 2. Theoretical Background

This chapter describes and explains details of the background knowledge for image verification process. This includes similarity measures and image comparison.

2.1. Similarity Measure

To find a resemble image that is stored in a database, matching process of the image has to extract features and contents of the image such as spatial layout, textures, colors or even shapes of image. Despite there are many similarity measures or descriptors, this research selects five well known descriptors to compare and evaluate their retrieval accuracy. This is the reason why this research chose the descriptors. Another reason is that the use of such descriptors covers analysis method for all possible features that can be extracted from normal image.

2.1.1. Auto Correlograms

Color correlograms are used to improve image retrieval accuracy of color histogram descriptor [3]. Color correlograms method accounts for the local spatial correlation of pairs of colors. The color correlograms of an image specifies the probability of finding a pixel of color j at a fixed pixel distance k from a pixel of color i in the image. Considering all the combination of pairs of colors, the size of color correlograms is $O(m^2 d)$ which is very large where; m is the number of colors and d is the distance between pixels.

J. Huang et al. [3] also proposed auto correlograms which is a subset of color correlograms. This approach describes only the spatial correlation between identical colors and the size of color correlograms decreases to be $O(md)$.

2.1.2. Color Histogram

Image retrieval uses color histogram as a common procedure [4]-[6]. The color is basic information of content that can be easily extracted from image.

This procedure represents the distribution of colors in an image uses color histogram. This color histogram procedure is extensively used in image comparing process. Generally, the computer uses RGB as colors to represent an image. The color is separated into several bins to store pixel counts within the range of color or frequencies of the represent colors [5]. Color Histogram is easy to compute and insensitivity to tiny changes in viewing positions. These are the advantages of color histogram. However, color histograms has drawback due to ignorance of the other information such as shape, spatial location, texture [2]-[3], [7]. Furthermore, the color pattern is not considered for the image. In other words, the different object contents of the two images are possible to contain same color histogram.

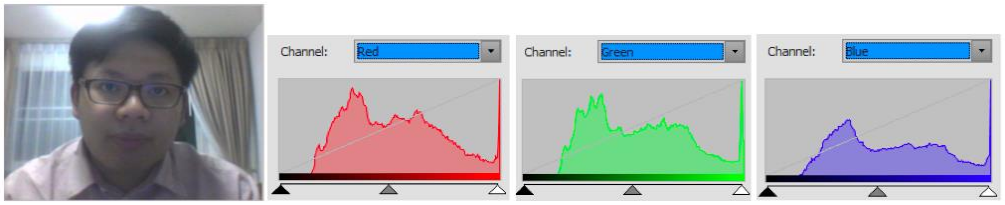


Figure 1. Color Histogram Descriptor

2.1.3. Color and Edge Directivity Descriptor (CEDD)

Color and Edge Directivity Descriptor (CEDD) is a descriptor that includes both texture and color information in a histogram which proposed by Chatzichristofis [7]. The color and texture of each block of image are extracted ant then are divided into predefined number. The structure of CEDD includes among six texture regions and each texture region consists of 24 color regions. The histogram is composed of 144 bins in accordance with the overall 144 color regions within six texture regions. For texture, six regions utilize to create from five types of edges as horizontal, vertical, 45 degree, 135 degree and non-directional edge. A part of color information is extracted from map color in each region to 24 preset colors by applying two fuzzy systems. A quantization is also used to define the color as three binary digits in the interval [3]. Therefore, the total size is limited to be 144 x 3 = 432 bits

or 54 bytes per image. The advantage of CEDD is the small size of the descriptor.

2.1.4. MPEG-7 Edge Histogram Descriptor (MPEG7-EHD)

The MPEG-7 is a visual standard for content description. This descriptor was designed by The Moving Picture Experts Group (MPEG) to provide standardized description for images or videos. MPEG has many types and MPEG-7 can be used independently from other MPEG standards. MPEG-7 is used to search image and video from allowed users or agents. It can be specified into several descriptors such as visual color descriptors, visual texture descriptors, visual shape descriptors, and motion descriptors for video. For example, users draw a few lines on the screen to get images that contain similar graphics or users describe actions to get a set of videos with similar actions [8]. In this research, MPEG-7 Edge Histogram Descriptor (EHD) was chosen. From Figure 2, MPEG-7 EHD consists of five types of edges that are vertical, horizontal, 45 degree, 135 degree, and non-directional edge which are represented in an image. The descriptor divides an image into 16 non-overlapping blocks of equal size and utilizes a 5-bin histogram to express the edge information of each image block [8]. The descriptor is scale invariant and supports rotation invariant and rotation sensitive matching operations [4], [8].

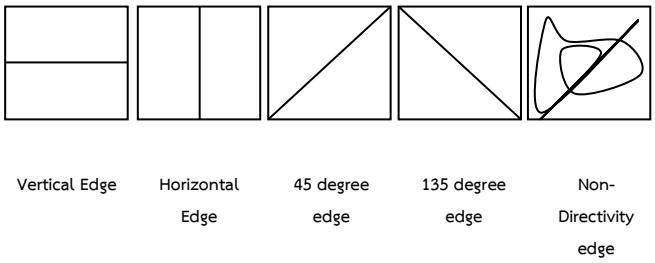


Figure 2. Edge Type in MPEG7-EHD Descriptor

2.1.5. Tamura's Texture

The significant feature to perceive an image for human is texture. Image has texture which is defined over a sub-image or region by grey levels instead of at a point [9, 10]. Tamura et al. [9] proposed six basic textural features

(coarseness, contrast, directionality, line-likeness, regularity and roughness). These textural features are measured by the psychological experiments to construct psychometric prototype as the computational measure. The textural feature performing better results than the others is coarseness which is the most essential factor in the texture.

2.2. Image detail

Two image types are described in this section. The first image type is a low-resolution image whilst the second image type contains the possible five conditions of face images collected by a digital camera.

A. Low-resolution image

A face image can be collected from a digital camera in various sizes. Some applications such as Image retrieval or Security Camera has methods for collected image into the database. Since the capacity of the storage is limited, image quality should be low-resolution image. Low-resolution of the image can be collected by specifying small size of image. The purpose of storing images of

Figure 3. Low-Resolution Image

a. b. c. d. e.

Figure 4. Regular Face Image and Face Image with Conditions.

a. Regular Face Image. b. Overexposed Face Image. c. Underexposed Face Image.

d. Non-frontal Face Image. e. Face Image with Facial Expression.

small size is to keep large number of images under the limited capacity of database. This image can be collected by normal digital camera. This method solves problem of network which might be not applicable with high-resolution image due to the limitation of speed. Low-resolution should be generated in suitable level that is independent of content change and condition of image. Comparing low-resolution image with high-resolution image has the challenge when image was collected from user's camera because most of input images have higher resolution than image in database. Therefore, larger image must be scaled into smaller image. After that the similarity measure was applied to such images with lower quality. In database of this research, the low-resolution image was captured with the resolution of 72 dpi with the RGB standard color and the intensity ranging from 0 to 255 on each pixel. The example of low-resolution image showed in Figure 3.

B. Image Condition

Real environment has some specific factors of face image that can affect the appearance of the image. These can be counted as conditions of the image. In this research, image conditions are separated into five types. The types of images considered in this research can be described as follows.

Regular face image

Regular face image is frontal-view face image without any condition. This type of image can be taken from any digital camera with any element of image. All elements include white balance automatically defined by the camera to adjust the image appearance similar to perception of human. Example of regular face image is shown as Fig. 4a.

Overexposed face image

The face image can be taken at brighter environment such as outdoor etc. This type of image, information of image is extracted in a difficult fashion. This type is called overexposed image. This type of image must be improved by setting the parameter of the image before start matching process operation and this

operation has to take some time to process. The matching process should have pre-processing to handle this problem without adjusting brightness of image to avoid operation time ingestion in pre-processing. In this research, the verification process based on five descriptors for matching image that applied to the overexposed face image which are collected by digital camera with +2EV exposure of brightness level from usual scene. The example of overexposed face image is shown as Figure 4b.

Underexposed face image

Underexposed image, the environment has insufficient light while taking image. Therefore, face images are darker and some content of the image will be loss when taking with this condition. The brightening process can solve this problem by applying to image before resizing but this solution takes some time to process. In this research, the verification process based on five descriptors for matching image that applied to the underexposed face image which are collected by digital camera with -2EV exposure of brightness level from usual scene. The example of underexposed face image is shown as Figure 4c. However, the suitable descriptor should support both overexposed and underexposed images with the same priority because these two conditions are significant conditions in the real situation equally.

Non-frontal face image

The frontal face image is regularly used for verification application. The frontal face image contains all image features with symmetrical information, i.e., eyes, nose, ear, and mouth. In case of non-frontal face image, the partial feature of face image is occluded when captured then it is the problem for verification process. The non-frontal face image has two types of pose variations, which are horizontal and vertical variations. The horizontal variation is the usual behavior of human so it can more occur than the vertical variation. This research focuses to find the descriptor which is the most suitable descriptor for this condition with the general limitation of face verification process as angle's range of pose

variation. This research supports ±45° horizontal variations that are used as a representative of non-frontal face image in figure 4d.

Face image with facial expression

Facial expression is personal emotion that was represented. Normally the image collected in database is regular face image without facial expression. However, real situation to verification face image of human can include face image with facial expression. Therefore, the image facial expression was selected to compare with low-resolution face image. This is a challenge task because the appearance of the image is difference. Facial expression has six main type of emotions, which are sadness, happy, anger, surprise, fear and disgust [11]. This research selects this condition to be a factor and it was used in verification process and the example was represented in the Figure 4e.

Chapter 3. Related Works

Since usages of online transaction are more widespread, security of the online banking systems should be the first priority to concern. For online transaction, there is a standard security for authenticating the transaction of online payment on Electronic Draft Capture (EDC) service and Online Payment service on the internet. However, most of the countries use their own network and servers to manage and secure the online transactions by themselves [12] instead of use such as a standard security or apply the online payment system to make more reliable and secure the online payment system.

3.1. Online Banking System

According to the flexibility, speed and efficiency, the internet became the main channel for communication between sellers and buyers. In this recent year, the internet is the main gateway that establishes usage of online banking system [13]. When mentioning about online banking system, most of persons think about online payment. However, Ali [14] described online banking system that users expected as Figure 5. Online banking is not the online payment, but also includes other processes that users expect from the online banking system. Figure 5 showed banking activities that were expected from users to be workable in online banking system. These banking activities include beneficiary payment, open account, monthly statements, balance enquiry, request checkbook, bank loans and etc.

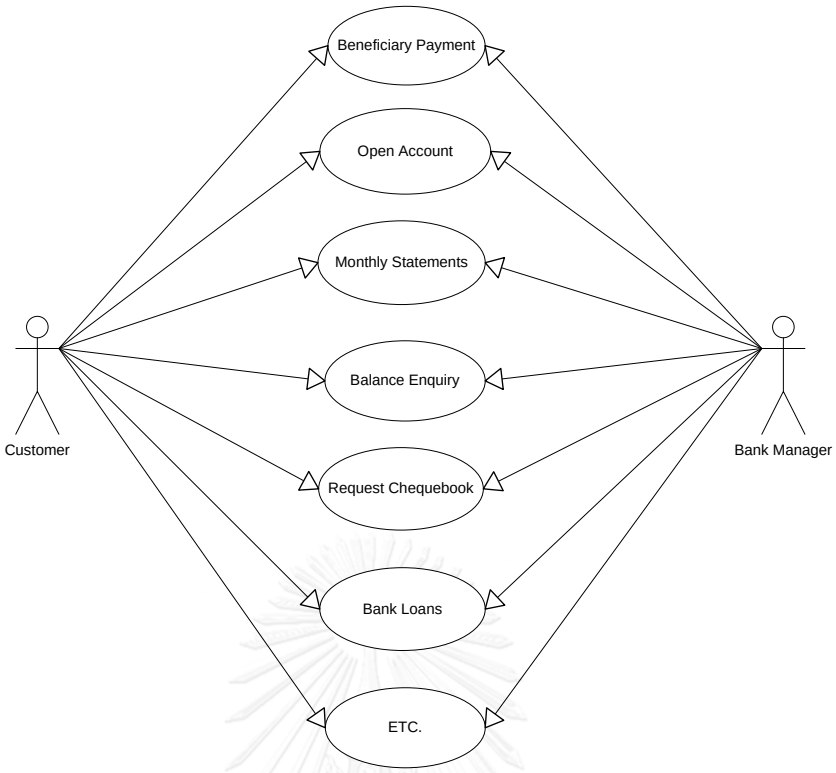


Figure 5. User Requirements of Online Banking System

However, there were limitations of online banking system. Ali [14] pointed out that many persons avoid using online banking system because of lack of awareness. The effectiveness of online banking system should be emphasized. Wrong assumption about transaction process is another reason. Someone thought that there might be extra charge of using online process. Security is still one of the important reasons that obstruct persons using online banking system due to leak of customer information and various sites cannot ensure that money will be safe online.

Since many banks tried to provide the best system with high quality which is fast, secure and safe to use, then many methods were invented to protect personal information of their customers [13].

3.1.1. **Credit card**

As credit card has played a crucial part in business for the last half of the century. Number of credit card users is still growing everyday as evidenced by

an increasing number of credit card holders and number of merchants accepting credit card. Many customers find out that credit card is a convenient method for buying stuffs and paying for bills at the end of period. Also, in merchants' point of view, credit card provides simply way to deal business with their customers across the world. Funds are generally paid to merchant within 48 hours through credit card network. This means that merchants and customers can make secure transactions without face-to-face communication [15]. Moreover, buyers are very convenient when using credit cards to pay for things in shops. Instead of carrying cash, buyers can carry only one credit card and do all payments. If something goes wrong, buyers will get a legal protection from credit card Company [16].

The well-known and world-wide credit card companies are VISA, MasterCard and American Express. The difference of these three companies is that VISA and MasterCard do not issue the cards by themselves. All transactions from credit cards of these two companies are processed between bank and merchant. They just manage the exchange of information among different financial institutions. Conversely, American Express issues its own card and does banking process [17]. To protect fraud transactions, each company uses almost the same security method to provide security for credit card as shown in Figure 6. VISA provides card security features by using signature panel, magnetic stripe, chip, card security code, etc. Each of these features has its own benefit [18].

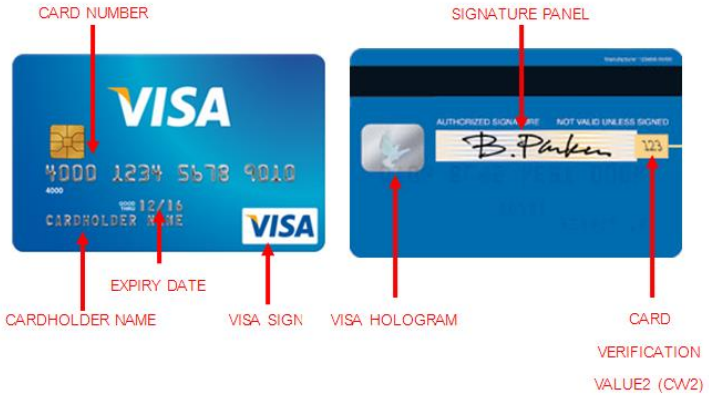


Figure 6. VISA Card Security Features

Security feature on a VISA credit card is a 16-digit account number or card number and cardholder name. On the back of the card, there are magnetic stripe, signature panel, and card verification value (CVV). Magnetic stripe encodes information of the card. Signature panel is a real signature signed by the owner of the card [18]. CVV or card security code (CSC) is a 3-digit code in magnetic stripe for a valid card. It is used to detect a counterfeit card. For the card security code, various card issuers use different names to indicate this security feature: CVV2 for VISA, card verification code 2 (CVC2) for Master Card and card identification data (CID) for American Express [17].

Figure 7. MasterCard Card Security features

On the other hand, MasterCard has almost the same features as VISA. American Express or even Discover have those security features as well. According to Figure 7 and Figure 8, credit cards from different companies have similar security features.

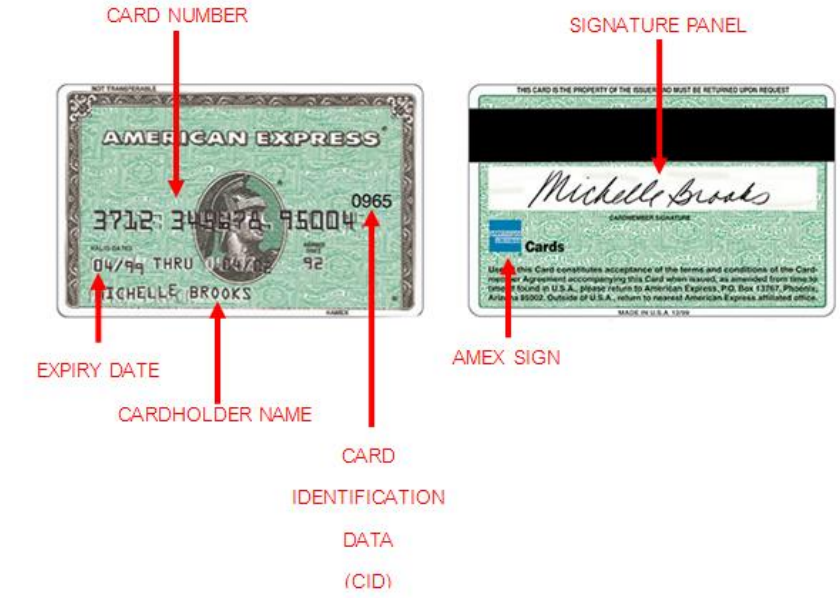


Figure 8. American Express Card Security Features

3.1.2. Security of online transaction via credit card payment

Online payment transaction is the process between buyer and seller on the online e-business system. Most of online payment transaction can be separated into two types, Internet Banking Payment Gateway and the payment based on the third party platform that is the direct payment mode. At this time, most users realize that bank online payment transaction system is a payment from buyer's account to seller's account directly, which is actually the second type of online payment transaction. However, this is not a way for the other banks or the other merchants that do not register with the bank system. Conversely, the bank's payment gateway system is a method supporting users to use the online payment transaction in various merchants [19].

Several methods are used to authenticate user in online payment transaction process. For example, the signature of user, Personal Identification Number (PIN) of credit card and one time password in SMS on mobile phone, etc. Each authentication method has its own advantages and disadvantages that will be described later. However, this authentication method can be separated by type of transaction.

Card present transaction

Card present transactions are transaction that both cardholder and card are presented at the point of sale. Merchants involved with this environment include stores and shop. Other unattended payment devices in some business such as gas station, self-checkout machine in supermarket also defined as card present merchants. In normal sales environment, merchants should take steps to assure that all components of transaction such as card, cardholder or transaction itself are legitimate.

VISA [18] has shown card acceptance process through magnetic-stripe card processing. According to Figure 9, the process starts with merchant who swipes the card through a magnetic card reader to request authorization of the transaction. Then merchant, to make sure the card is valid, must check all features on the card and security element. After obtaining authorization, cardholder signature must be signed on the transaction receipt. Merchant should compare signature on the card with signature on transaction receipt carefully.

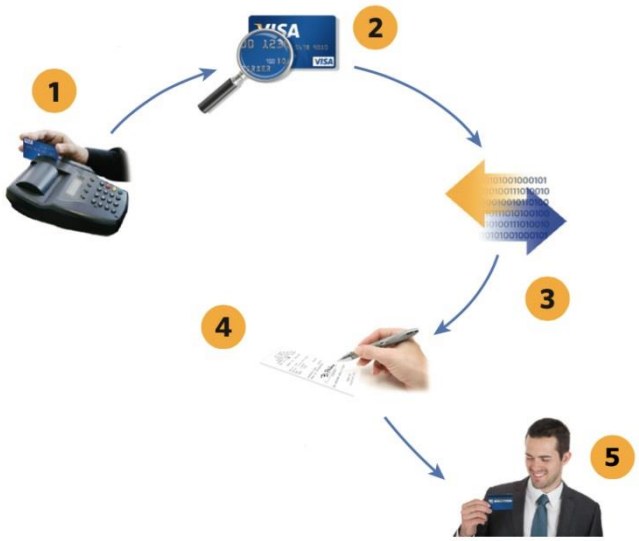


Figure 9. Illustration of Card Acceptance (Magnetic-Stripe Card Processing)

TD Merchant Services [20] also suggested about signature method that merchant should compare signature from customer with signature on signature panel. Spelling and handwriting should be checked carefully. For the method that uses the digital signature, the advantage is that giving a signature is a simple process for user. However, the disadvantage is that the system has to add extra device such as a signboard machine to get signature data and signature can be easily stolen [6].

Another card acceptance process is through Chip Card Processing. From Figure 10, merchant requests transaction authorization by asking cardholder to put the card into chip-reading device. Then the transaction will require PIN-Verification, card holder should enter the PIN. The drawback of this method is that merchant does not have opportunity to examine the card [18]. Another drawback is its reliability. Murdoch et al. claimed that attackers may perform a man-in-the-middle attack to trick the host of transaction so that the PIN is verified correctly while the card is used without entering the PIN [12].

Figure 10. Illustration of Card Acceptance (Chip Card Processing)

Card not present transaction

The growth of e-commerce channel leads to the increasing numbers of situation where merchants are processing transaction with absent card and cardholder. In this situation, fraud may be very difficult to detect. Therefore, card acceptance procedures for this kind of transaction should be different form card present transaction procedure. Despite procedure must still be able to verify by merchants for identity of cardholder and validity of purchase.

Authentication method for card not present is using card verification method. The card verification method is a 3- or 4-digit number printed on the card but not consisted in magnetic stripe. Since the number is not contained in magnetic stripe, it cannot be copied by skimming. These security features has different name for VISA is CVV2, MasterCard is CVC2 and CID for American Express (Figure 6-8). This can help merchant to ensure that person who makes the transaction is the owner of the card [21]. However, if the card has been stolen then One-Time-Password (OTP) and Static Password is another process that can help protecting the card [17].

One-Time-Password (OTP) is a unique secure code that bank generates and sends to cardholder when processing online transaction. OTP will be sent via

SMS on registered mobile phone number [22]. Figure 11 showed OTP requested screen when customer tried to process transaction.

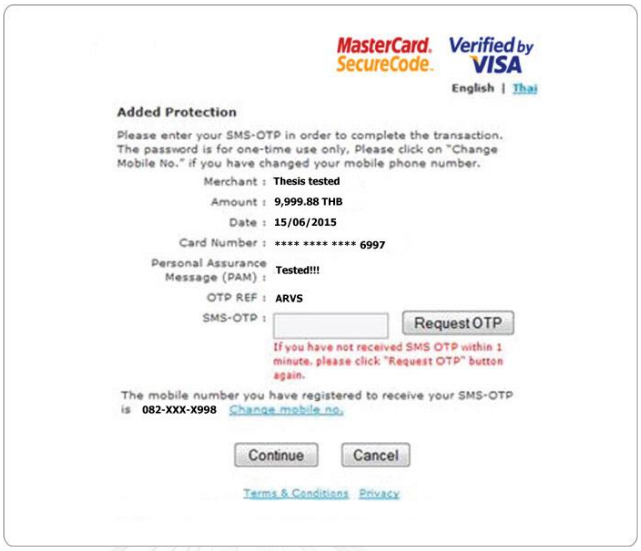


Figure 11. One Time Password Request Screen

However, there are still weaknesses of this method. It is not robust to malware-based reply attack, phishing attack, and malware based impersonation attack [23].

Sometimes, Static Password is used to authorize transaction. From Figure 12, American Express requires “Safe Key” from user to process transaction. On the other hand, VISA requires “Password”. These two things are the same which is Static Password. It can help validate for the real cardholder. However, the Static Password can be lost, stolen, forgotten or disclosed. Intimates or colleagues can easily access password. If static password leaks to another person, then transaction can be authorized for card not present transaction. These are the drawbacks of this method [24].

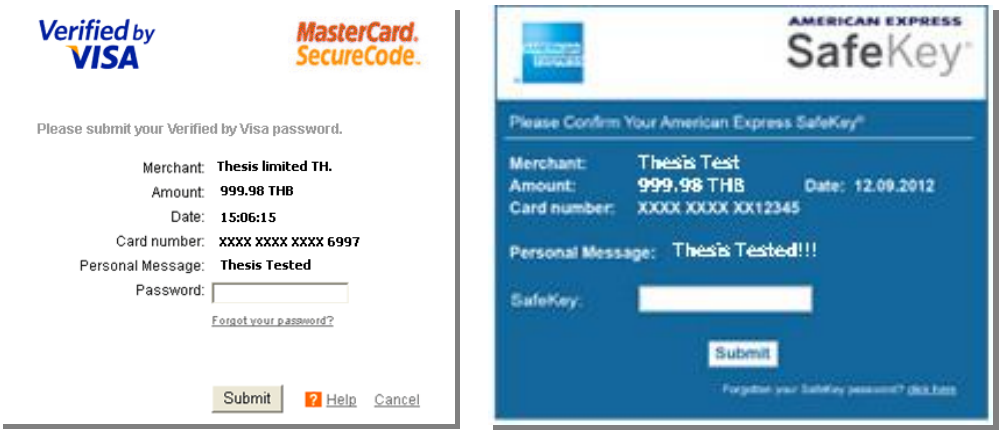


Figure 12. Personal Identification Number Request Screen

Some authentication methods verify transaction by using the encrypted picture that is hidden in the credit card. However, the limitation of this method is the picture size. The size is too large to be stored in the card. Moreover, the picture might be simply copied to other users or attackers [25]. Some country prefers to make more reliable system by using the biometric data from the center of government. For example, in Turkey, credit card payment transaction utilizes the biometric information embedded in ID card to verify the person who makes a transaction [12]. However, this methodology was scoped to support standard of each country. Obviously, such a scheme cannot apply to the other transaction standards [12].

For all methods that have been mentioned, it can be assumed that, the person who makes transaction is not the same person with cardholder. A transaction can be processed if the person who makes the transaction knows PIN or able to sign a signature. Therefore, authentication process has been researched and developed into new systems that are more reliable and supports the online transactions such as using fingerprint as a biometric authentication for both card presented and card absented transaction.

3.2. Biometric for Verification

The demand to authenticate personality for machines is increasing every day. Persons are searching for the most suitable and secure method to protect themselves when making an online transaction. Biometric can identify and proof for the real person. The term of biometric has been described in [26] as "*the thing that used for the study of automated methods for identification or authorization of individual using physiology or behavior characteristics.*"

According to Phillips [27], Biometric identifiers are important because these identifiers can show identity of the person. As mention before the important of biometric systems are increasing, most of systems start to search for better way to implement biometric into their systems. Phillips [27] also points out that biometric identification becomes a key technology that can help user to reduce fault access in electronic commerce. However, precision of identification and authentication is very challenging. Primary advantage of using biometric identifier over other methods is that they really do what they should, *identify for user*. This method uses real characteristics to authenticate users. There are many techniques for biometric identification such as iris scanning, fingerprint scanning, speech recognition as well as face recognition. It can be noticed that all biometric, fingerprints, iris, speech or faces are permanent and not easily to change. Moreover, most of biometric techniques are something that cannot be forgotten or lost. This advantage is suitable for both users and system administrators because resources associated with reissued card/password/PIN can be avoided. By resources, these covers time for issued processes, cost spending, cost for system management and anything that involves [24].

For biometric can be work effectively, it should have four properties (1) universality: all identify population should possess the biometric; (2) uniqueness: biometric should be different from all population; (3) invariance: all biometric should remain the same since collected; (4) resistance: for potential countermeasure biometric should be resistant [27].

3.2.1. **Biometric Identification**

Iris scanning

Iris is annular region of eye bounded by white of eye (sclera) and pupil. Iris texture is very complex and distinctive information. Each iris from different person is distinctive, like fingerprint [28]. Saini and Rana [29] mentioned that iris recognition is one of the most secure for recognition and authentication. This technique becomes very useful because it is one of the most accurate technologies that has low rejection rate with low false acceptance as well. Once iris has been taken using standard digital camera, authentication process are comparing present subject with stored version [29]. Only a few seconds on millions of records in database, iris from live image was compared to previous kept ones to seek for the matching. Threshold for this decision is taken from amount of iris data that are visible. Despite it sounds very secure, quick and easy, some iris is being corrupted by reflection or contact lens boundaries [30]. Moreover, cost of iris recognition machine is very high. The systems also require considerable user participation [28].

Speech recognition

Voice is a biometric obtained from both physiological and behavioral aspects. In term of physiological aspect, voice from individual person is based on size and shape of appendages such as mouth or lip that use to synthesis of the sound. This physiological aspect of human characteristic creates characteristic for individual person. On the other hand, behavioral aspect makes each person speech change over the time. Ages, emotion or even medical conditions such as cold can make voice slightly distort [21]. Speech recognition is the only one biometric technology that does not verify visual feature of human body. This method recognizes sound vibration of individual person and compares it to existing voice sample. User is usually required pronouncing some words or phrases [30].

However, [31] suggested that voice is not a very distinctive and may not be suitable for identifying person in a large scale. Speech recognition is very sensitive to factors such as noise surrounding. These drawbacks are supported by [29]. Moreover, voice may be hacked with recording voice massage and needed a lot of processing time to distinguish voice from different person.

Fingerprint scanning

For many centuries, fingerprints have been used as personal identification because of the accuracy of matching process [32]. A fingerprint is pattern on surface of fingertip. Cost of fingerprint scanner is not expensive comparing with another biometric scanner [28]. Even using fingerprints in identification process costs less than that of iris recognition. However, fingerprint can be copied. Form Figure 13, fingerprint can be copied by using plastic sheet to duplicate 3-dimensional fingerprint [33].

Figure 13. Fake Fingerprints Copied

Source : Prabhakar, Pankanti and Jain, "Biometric Recognition: Security and Privacy Concerns",2003

Fingerprint is the biometric information that is unique enough to use in security system but the authentication process needs a sensing device to process the online transactions [34] Moreover, the fingerprint yields a fault interpretation caused by dryness or dirtiness of finger's skin or by age. In a term of resolution, fingerprint is captured in high-resolution corresponding to need of memory space [35]. Jain et al. [28] also supported the reason of interpretation. As fingerprint is a surface of fingertip genetic factors, environment or aging is an important factor that can affect the authentication process.

Face recognition

According to the FERET database [36], in half pass decade, face recognition has become a considerable area of computer vision. Face recognition is a method to evaluate facial features. It is an application that determines individual by comparing a digital image with images in database [29].

Saine and Rana [29] also mentioned many advantages of face recognition. Face recognition requires less cooperation of test subject to due process and does not require direct contact from users to verify themselves. This leads to clean environment for monitoring and can be counted as a contactless system. System can be set up in any place and be workable among massive crowd. Face recognition has more key advantages than other identification. If comparing face recognition to other techniques, major prominent point of this technique is that it is non-intrusive. In order to collect data which is face detection, it requires less cooperation or modification of normal behavior from user to collect useful data [26]-[28], [37]. Phillips [36] also claims that the result of face recognition are shown in a large number of papers that recognition results usually correct more than 95% on limited-sized database.

In order to assure face recognition system is acceptable, it should follow these issues. Firstly, face should be detected in a acquire image. Secondly, face should be located in an image. Thirdly, face should be detected from general viewpoint or any pose [28]. . However, this research focuses only on applying the comparison between face image captured by user's camera and low-resolution image retrieved from the database of limited capability [38].

3.2.2. Face Matching Verification

As mentioned before, biometric use individual physiology to identify person. Authentication technologies that use biometric such as fingerprint, face or hand are available and already in use [39]. A biometric system is recognition system that operates by getting data of biometric from individual, extracting features of data and comparing with templates in database. Moreover,

biometric system can separate into either identification or verification mode [40].

Identification mode was operated through system that recognized image by searching from all templates in database for matching image. In this mode, system conducted one to many comparisons. Conversely, verification mode was operated through system that validates identity by comparing acquisition biometric data with same person biometric template in database. System conducted one to one comparison and determined for YES or NO. This verification method can prevent multiple persons using same identity [41].

Normally, there is a module of biometric system for matching verification. Matyas and Riha [25] proposed biometric system that can be adapted with the proposed process of research. Basic components of the model are shown as Figure 14.

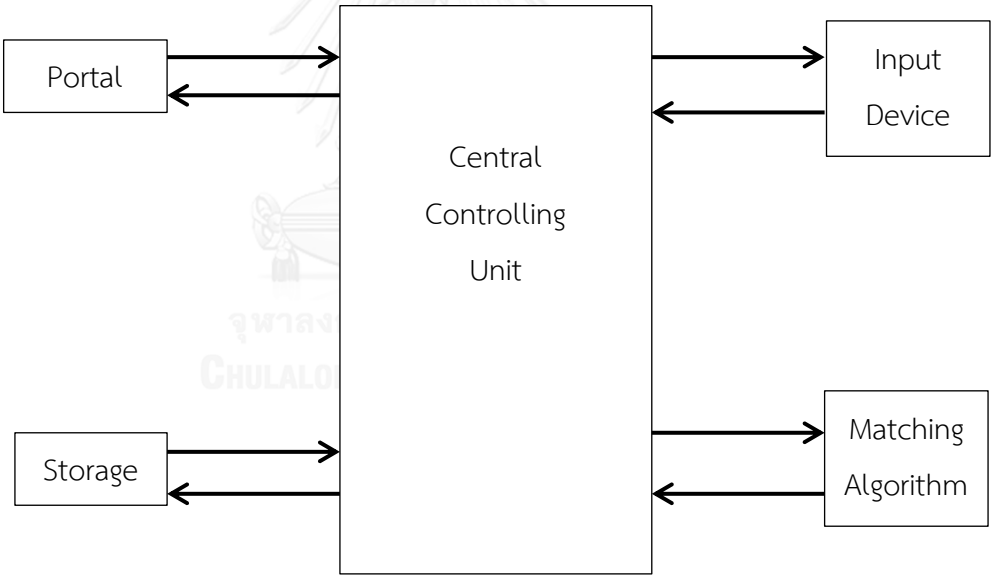


Figure 14. Model of Biometric system

Portal is a component to protect authorization process. This portal is the first step to start the verification process.

Central controlling unit helps system to control all processes and return result of verification.

Input device acquires biometric data from user.

Storage of biometric data is similar to the database that keeps all biometric templates. Link between users and their biometric data must exist.

The Matching Algorithm is the algorithm that compares and verifies current biometric feature with template that was stored in database. In this step, desired threshold is needed as accuracy measure and determines whether the system should process the next step. In this case, the result was stated as YES or NO. This matching algorithm was supported by Hosseini and Barkhordari [42]. Definition of matching algorithm was stated in [42] that it is *"the comparison of biometric templates used to calculate their degree of similarity or correlation"*. Moreover, in verification process, threshold value should be calculated. This number can be used to define degree of correlation of each image and is necessary for comparison process.

For biometric matching verification, Kim, Kang and Chang [43] suggested about using fingerprint as a biometric system to verify identity. Fingerprint verification system is similar to module of biometric system in Figure 14. Also, verification method has been suggested as one to one matching. This method can optimizes search technology from many persons in database.

Prabhakar et al. [33] have suggested about applying biometric system into the application. Application that might use biometric falls into 3 main groups. Firstly, commercial application such as ATM, Credit card, medical record, and computer network log-in. Secondly, government application such as passport control, and nation ID Cards. Lastly, forensic application such as criminal investigating and parenthood determination. For commercial application like ATM, most persons set password to a date that they easily remember. These passwords are as easy to remember as crack. Therefore, biometric identification can support in this situation.

Chapter 4. Proposed Method

4.1. Overview of Research

According to the objectives, the research part I was studied to ensure that MPEG7-EHD worked well in the authentication process. After that the proposed process of the online transactions with face authentication method was developed to enhance the authentication method of online transactions. Finally, the authentication process based on research part II was compared with the traditional approach.

4.2. Research Part I Approach

In research part I, the most suitable descriptor for face matching verification was sought. MPEG7-EHD was compared with others descriptors. To do the experiment, 11 persons were used as a sample group. Images of each person were kept under five conditions: normal, darkness, brightness, facial expression, and non-frontal face image (Figure 4). Five image conditions were compared with low-resolution image (Figure 3) using IMG (rummager) [44].

Experiment was separated into two parts:

1. Compare process between same person images, this process compared low-resolution image and image condition of each person. This part calculated the average of distance $\overline{d_{s1}}$ between two images from the same person.
2. Compare process between low-resolution image and image condition of different person. This part calculated the average of distance $\overline{d_{s2}}$ between two images from the different persons.

4.3. Research Part II Approach

This research proposed more secure authentication method for online payment process. Proposed method was created as the proposed process by Visual Basic.NET. The proposed process was created from the result from part 2 of the questionnaire. 220 persons were involved in this step. The proposed process simulated online payment process for both EDC and OTP. Face matching verification was applied into the proposed process to replace traditional verification process for security reason. For accuracy of the proposed process, threshold in matching verification process was calculated in K-fold fashion [45]. This step used 100 persons as a sample group to calculated distances to use as thresholds.

After that, questionnaire was handed to 35 persons before and after testing the proposed process. Performance of online payment process was evaluated. Hypotheses were set for statistical analysis. This research used statistics to analyze data.

4.4. Data Collection

According to Hox [46], there are many strategies to collect data (e.g. experiment, survey, interview, and etc.). To begin with experiment, researcher assigns a treatment group and observes for respond. This method allows causal inference but take a lot of time to analyze. Second is survey, questionnaire is used in this strategy. In order to collect huge number of data, quantitative approach should be applied. Third strategy is interview method, qualitative data is collected by in-depth interview and results are analyzed in further step.

In this research, survey method using questionnaire was conducted to collect data from sample persons who attended the security process [47].

4.4.1. Data Source

4.4.1.1. Primary data

Primary data in this research was separated into two parts. Data was collected form questionnaire and in-depth interview. In this research, quantitative approach was used as method to collect data. All data was analyzed and used to determine whether the proposed process has better usability and performance or not.

Face images are important primary data as well. The images were used in Research part I for finding out the best descriptor. For Research part 2, face images were used when calculated threshold for proposed process.

4.4.2. Sampling Method

This research collected quantitative data. For the proposed process, 100 persons were asked to collect face image. Part 1-2 of questionnaire were published and sent randomly to 220 persons to collect information and answers. After proposed process was created, the specific 35 persons sample group was asked to evaluate performance of traditional online payment and the proposed process.

In this research, it can be noticed that convenience sampling and purposive (or judgmental) sampling were used. Saunder et al. [48] mention that convenience sampling is the easiest method to collect samples but it can cause uncontrollable bias because samples are selected randomly. The convenience approach was used in collecting face image step for the proposed process and part 1-2 of questionnaire. After that purposive method was used to select 35 persons sample group that were suitable to answer research questions and achieve the objective.

4.5. Questionnaire Design

To fulfill the third objective, questionnaires were created following the advice of four experts. Questionnaire contained four parts. All items in questionnaire were reviewed and verified by four experts. The name and affiliation of each expert is shown in Table 1.

Table 1 Experts Information

No.	Name	Position	Company
1	Mr.Nattakan Praprutdee	Assistance Vice President	Kasikornbank Co.,Ltd.
2	Mr.Niphon Sinsawad	Assistance Unit Manager	Kasikornbank Co.,Ltd.
3	Miss Supaporn Arpacharudkul	Business Area Manager	IBM Solution delivery Co.,Ltd.
4	Miss Jutamas Limsirinawa	Technical/Analyst Leader	IBM Solution delivery Co.,Ltd.

Questionnaire was separated into 4 parts as mentioned before:

i. Part 1 asked about general information of person who filled the questionnaire.

ii. Part 2 focused on problem from traditional online banking system. The answers from this part were used as requirements for a new proposed process. Questions in this part are derived from everyday security problems that sampling group had been faced and had been approved to be suitable questions from experts.

iii. Part 3 focused on Usability, Capability and User satisfaction from traditional process. This part of questionnaire used four-point scale to collect data for the third objective of this research.

iv. Part 4 was similar to part 3, but it focused on Usability, Capability and User satisfaction after using the proposed process. Four-point scale was utilized to collect data for objective 3 of this research as well. Also, some comments were added as suggestion from experts.

4.6. Proposed process Design

In this research, the proposed process was created based on some parts of traditional process. There are two proposed processes for both EDC process and OTP process.

The proposed process supposed to do online payment process with face matching verification. Main functions of EDC and OTP process are almost the same which are online payment and verification process. However, for EDC process, both merchant and customer interact with payment process as shown in use case diagram in Figure 15. Conversely, for OTP process only customer interacts with payment process as shown in Figure 16.

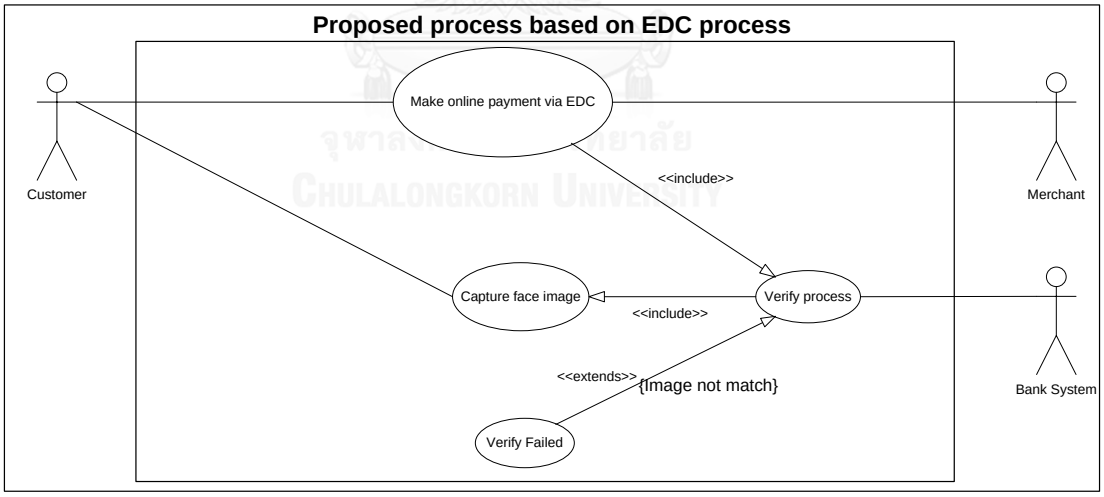


Figure 15 Use case Diagram of Proposed process (via EDC)

Use case descriptions of proposed process based on EDC process was described on each use case as follow:

1. **Use case :** Make Online payment via EDC

   Related Use cases:

   Generalizations of:

   - Verify process

   Steps:

   - Customer fills in information
   - Customer chooses start payment
   - Bank system responses by displaying simulation screen
   - Customer gives card to merchant
   - Merchant swipes card and enters amount

2. **Use case :** Capture face image

   Related Use cases:

   Generalizations of:

   - Verify process

   Steps:

   - Bank System activates face matching verification process
   - Customer captures his/her own image

3. **Use case :** Verify process

   Related Use cases:

   Specializations of:

   - Make online payment via EDC

   Steps:

   - Bank System responses the result of verification

4. **Use case** : Verify Failed

   Related Use cases:

   Extension of:

   - Verify process

   Steps:

   - Customer is requested to re-submit transaction

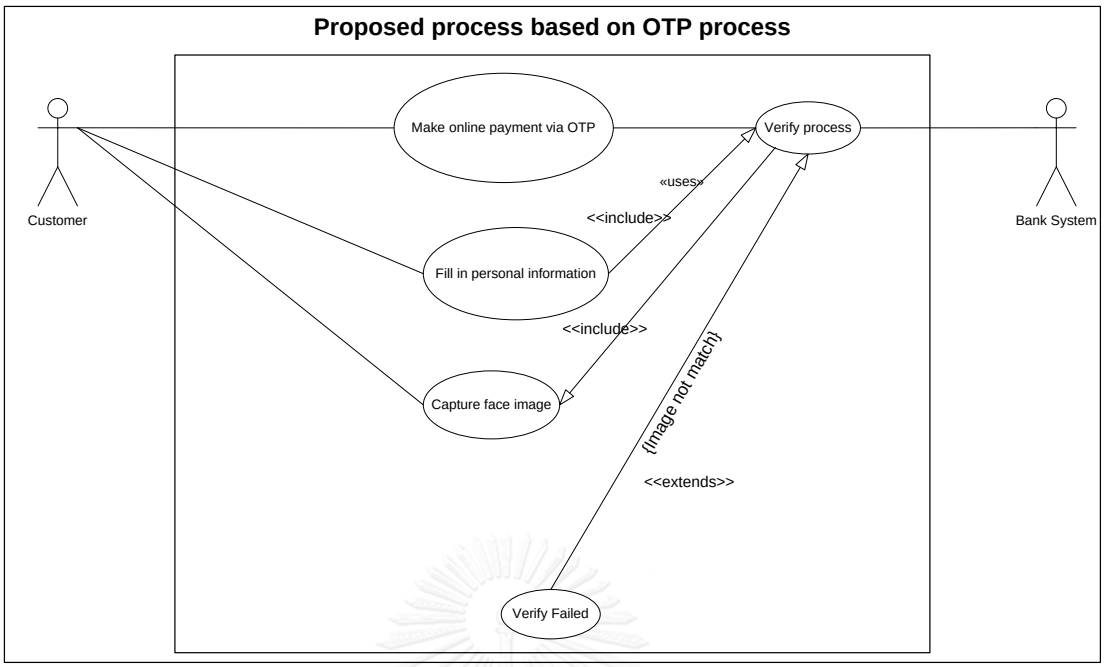


Figure 16 Use Case Diagram of Proposed Process (via OTP)

Use case descriptions of proposed process based on OTP process was described on each use case as follow:

1. **Use case :** Make Online payment via OTP

   Related Use cases:

   Generalizations of:

   - Verify process

   Steps:

   - Customer fills in information
   - Customer chooses start payment
   - Bank System responses by displaying payment screen to require personal information

2. **Use case :** Fill in personal information

   Related Use cases:

   Generalizations of:

   - Verify process

Steps:

- Customer fills in personal information
- Customer presses submit button

3. **Use case :** Capture face image

   Related Use cases:

   Generalizations of:

   - Verify process

   Steps:

   - Bank System activates face matching verification process
   - Customer captures his/her own image

4. **Use case :** Verify process

   Related Use cases:

   Specializations of:

   - Make online payment via OTP

   Steps:

   - Bank System responses the result of verification

5. **Use case** : Verify Failed

   Related Use cases:

   Extension of:

   - Verify process

   Steps:

   - Customer is requested to re-submit transaction

Payment process based on EDC of traditional method was compared to payment process based on EDC of the proposed process as displayed in Figure 17. The payment process based on EDC of the proposed process changed verification step from signature verification (manual process) to face matching verification.

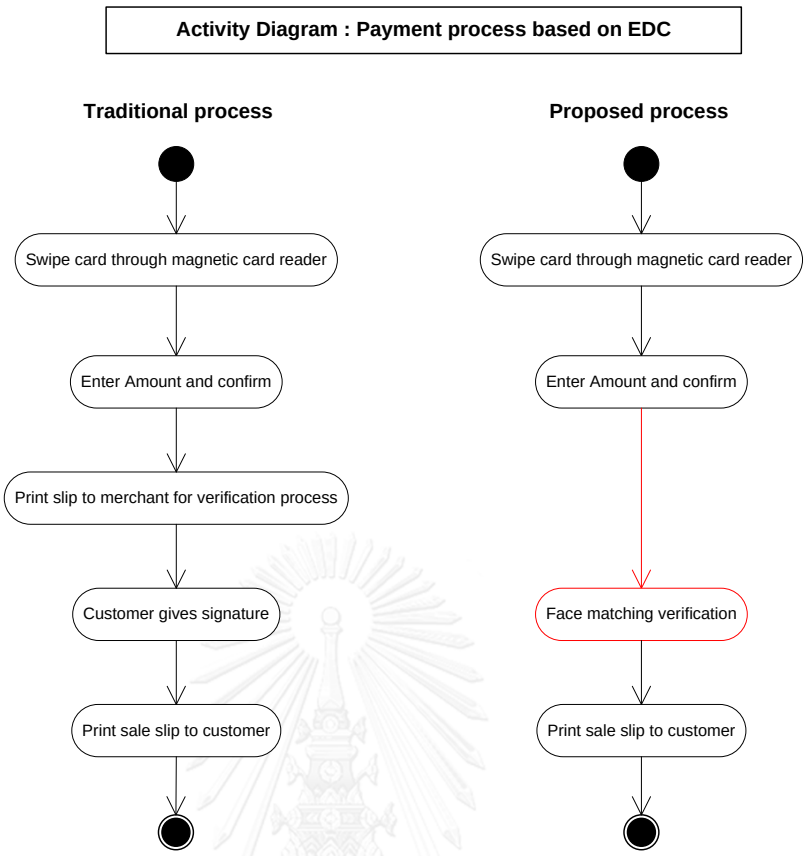


Figure 17. Activity Diagram of Traditional Process compared with Proposed Process (via EDC)

Design step of the proposed process is shown that most of steps remain the same as those of traditional process. However, the proposed process was designed to reduce pay in slip printing step and signature request in verification step was replaced by face matching verification process. The proposed process was designed to simulate enhancement of security process from traditional online payment. The expected screens of the proposed process are presented in Figure 18-20.

When customer fills name and surname, the system retrieves an image of the customer that is stored in the database to display at right side of the proposed process. Name and surname are the link between user and his/her biometric data as mentioned in Chapter 3.

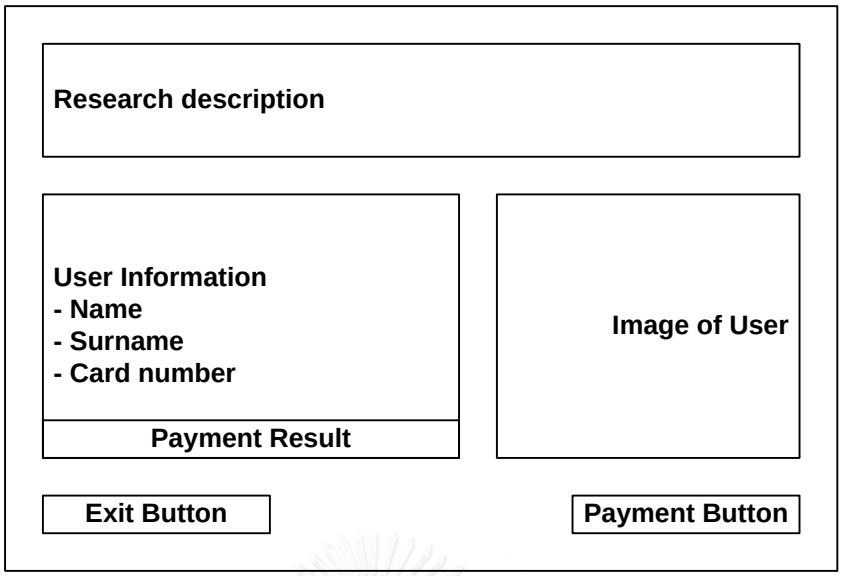


Figure 18. Pre-processing Payment Method based on EDC

Before continuing to the payment step, simulation step of EDC was designed as shown in Figure 19. In this step, camera was activated to acquire biometric data.

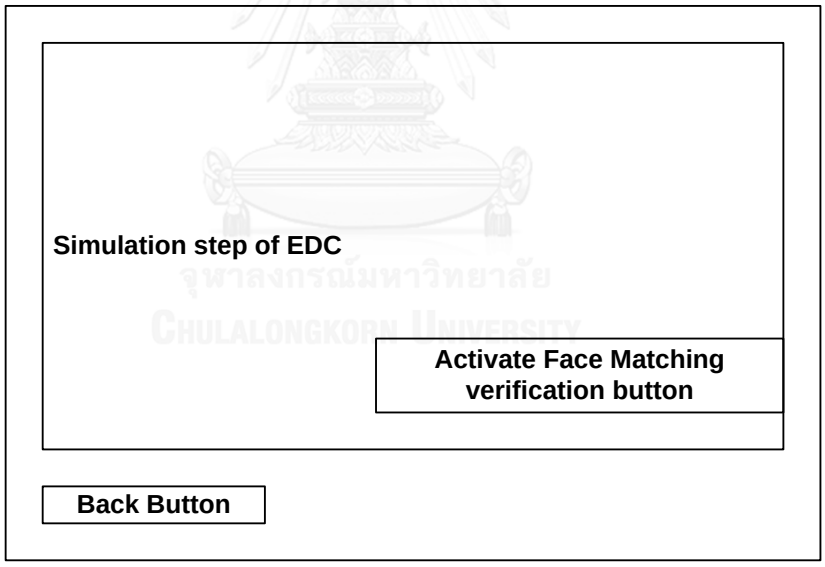


Figure 19. EDC Payment Simulation

The proposed process was designed to capture customer's face from web camera and process face matching verification as shown in Figure 20. After that approval result was shown at left side of the proposed process in Figure 18.

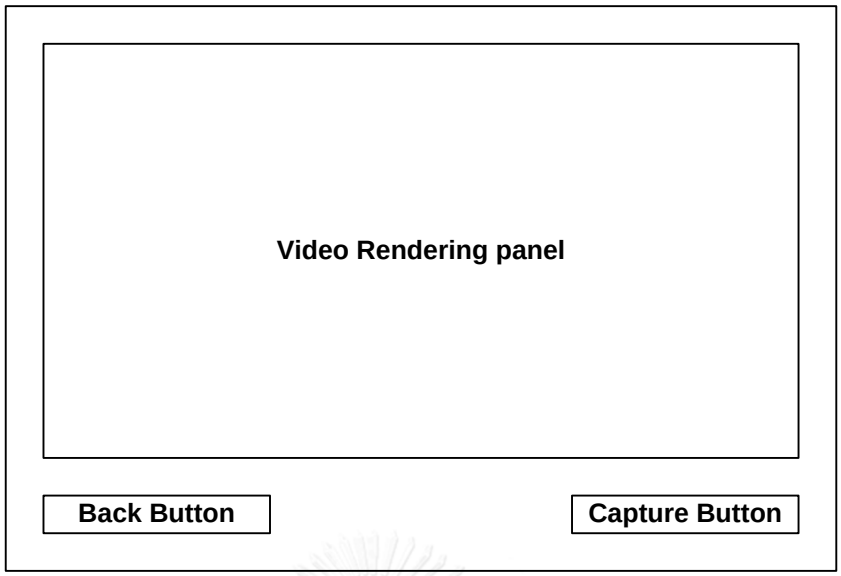


Figure 20. Face Matching Verification Method Based on EDC

For the online payment based on OTP password, the second proposed process was created to simulate the situation of online payment as same as traditional process. However, the verification process was changed from OTP verification to face matching verification process. Steps of the traditional OTP process and the proposed process are show in Figure 21. Screens of the proposed process are presented in Figure 22-24.

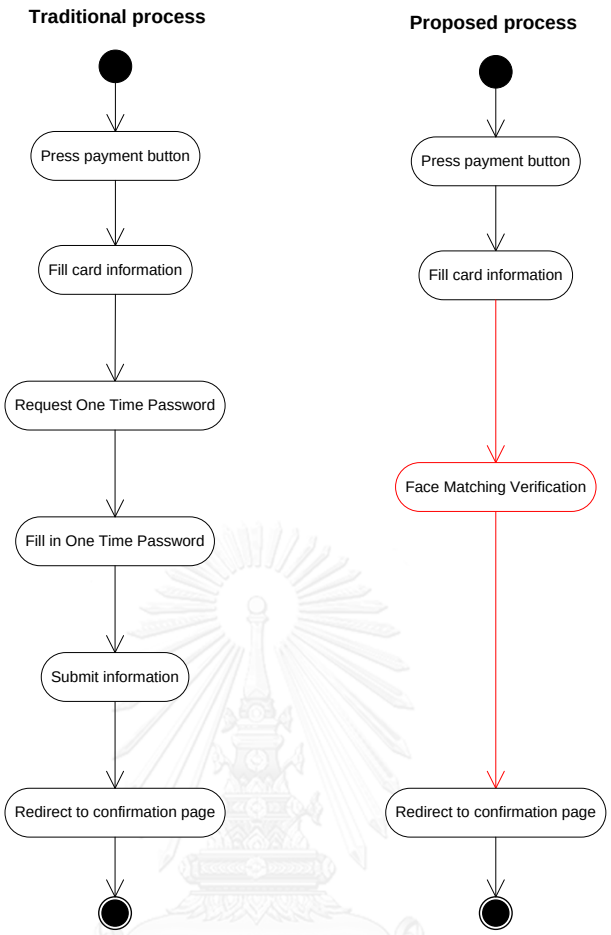


Figure 21. Activity Diagram of Traditional Process Compared with Proposed Process (via OTP)

The proposed process design for OTP process is similar to EDC as shown in Figure 22. Customer is requested to fill name and surname to get his/her image from database.

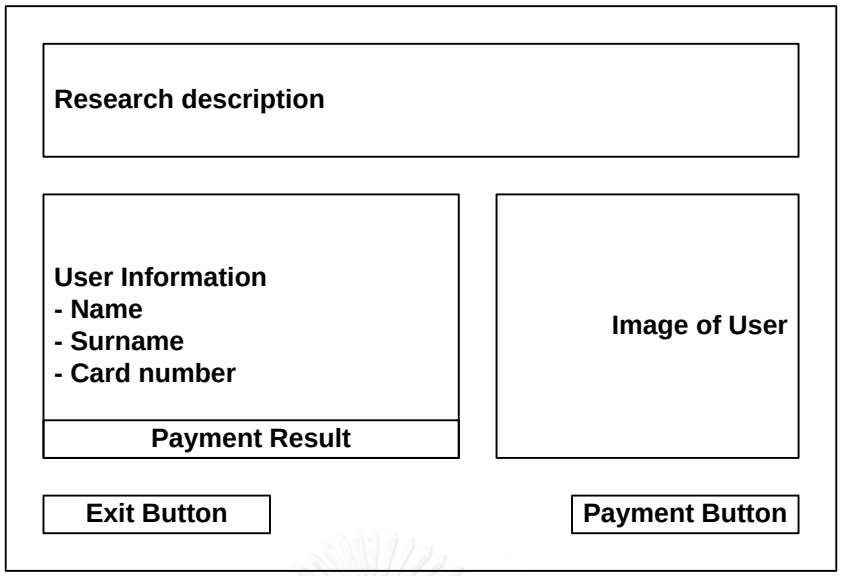


Figure 22. Pre-processing Payment Method based on OTP

For OTP process, the proposed process was designed to simulate OTP payment by asking customer to fill some information of credit card as shown in Figure 23.

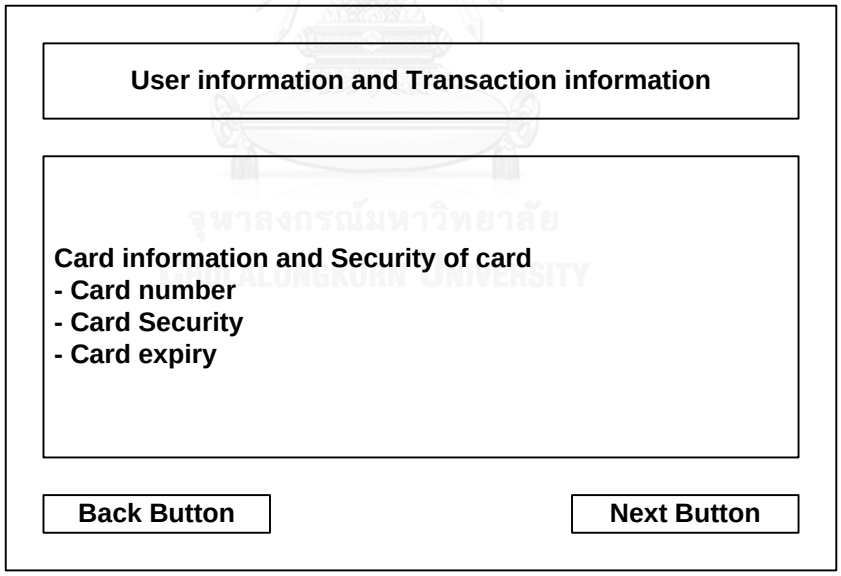


Figure 23. OTP Payment Simulation

Face matching verification process was designed to use instead of OTP request step. After face was verified the proposed process was requested to authorize automatically as shown in Figure 24. After that approval result was shown at left side of the proposed process in Figure 22.

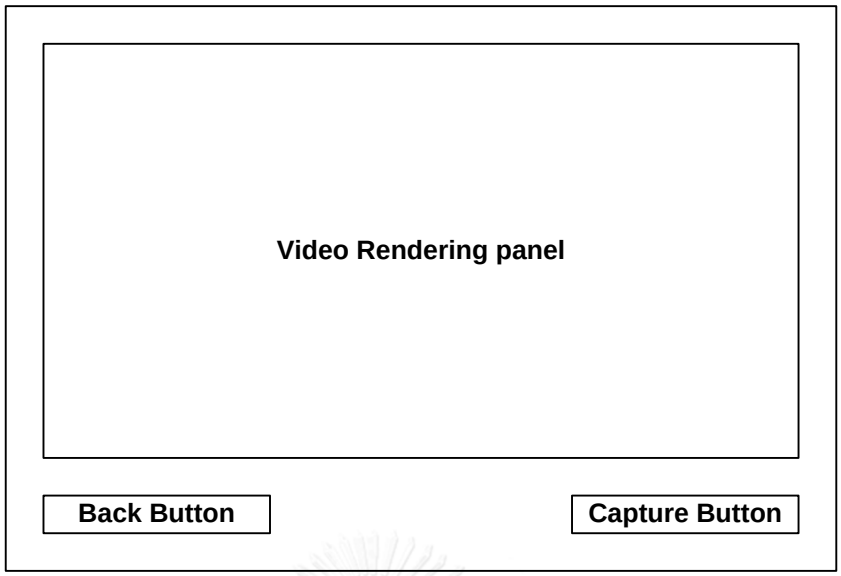


Figure 24. Face Matching Verification Process

4.7. Data Analysis

To fulfill the first objective, MPEG7-EHD was compared with other descriptors using IMG(rummager) to calculate distances between low-resolution face image with five conditions face image [36]. After that the distance values were used to find out threshold value. Then accuracy of threshold value was calculated as the Harmonic means to analyze the results and search for suitable descriptor [38].

For the second and third objectives, results from part 1 and part 2 of the questionnaire were analyzed. These results can be analyzed and used as a challenge and barrier for the proposed system. Therefore, the proposed process was created following results from part 2 of the questionnaire to eliminate problem that occurs during traditional process. The results from part 3 and part 4 of the questionnaire were analyzed by statistics. For statistical analysis, this research uses T-Test with 2-tailed analysis. A hypothesis was set for each question in questionnaire. Primary data was used for the result discussion.

Chapter 5. Experiments and Results

This research can be separated into two parts. Research part I was studied to ensure that MPEG7-EHD worked well in the authentication process. Then research part II, the proposed process of the online transactions with face authentication method was developed to enhance the authentication method of online transactions. Finally the proposed process was compared with traditional process by statistical method.

5.1. Research Part I Experiment and Results

The research part I experiment, specification of both software and hardware was predefined in this research. For hardware, DSLR digital camera with lens 18-135mm was mainly used to collect the dataset of images of size 3456x5184 pixels with five conditions as mentioned. Moreover, the low-resolution camera with resolution of 0.3 megapixels embedded in digital mobile phone was prepared to collect the images with low-resolution of size 180x180 pixels. For software, IMG(rummager). *"A program for calculating image distance"* developed by Chatzichristofis et al.[44] was applied for face matching.

Images in this experiment were captured from 11 persons by both high-resolution camera and low-resolution camera. For high-resolution, all image conditions are Regular faces image, underexposed face image, overexposed face image, non-frontal face image and image with facial expression. These images used for comparison process with low-resolution image by IMG(rummager) program on each descriptor resulting in a distance value. Therefore, the low distance between two images can be indicated that they are similar images. Consequently, this research can be separated into two parts for comparison process. The first part is comparison between two images of the same person. This process

compare between low-resolution image and high-resolution image with one of five conditions of each person. This part calculates the average distance $\overline{d_{s1}}$ corresponding to difference between two images of the same person. On the other hand, Second part is comparison between low-resolution image and high-resolution image with one of five conditions of any of two different persons. This part calculates the average of distance $\overline{d_{s2}}$ corresponding to difference between two images of different persons. After that the mid-point of these two average values was calculated as

$$d_{mid} = \frac{\overline{d_{s1}} + \overline{d_{s2}}}{2} \quad (1)$$

Then, the standard deviation(SD) of all distances was calculated to find out the appropriate range of threshold used for indicating which face image with conditions belongs to that person. The 21 threshold values were considered starting from $d_{mid} - SD$ to $d_{mid} + SD$ with step size of $0.1SD$ orderly. Each value of threshold was used for comparison process of low-fresolution face image and the face image with condition. If the distance between two images is less than the selected threshold, then the image with condition will be accepted as a verified person. Contrarily, the condition image was rejected. After that, this research calculate the False Rejection Rate (FRR) and the False Acceptance Rate (FAR) as follows.

$$FRR = \frac{the\ number\ of\ false\ rejections}{the\ number\ of\ comparisons\ in\ two\ images\ of\ the\ same\ person} \quad (2)$$

and

$$FAR = \frac{the\ number\ of\ false\ acceptions}{the\ number\ of\ comparisons\ in\ two\ images\ of\ different\ persons} \quad (3)$$

Both the FRR and the FAR value showed the performance of verification system. The low value of FRR and FAR represents the higher system performance.

However, for the best configuration in this research, the harmonic mean of these two rates was calculated as follows.

$$H = \frac{2 \cdot FRR \cdot FAR}{(FRR + FAR)} \tag{4}$$

The most suitable threshold of each person is the value that gives from the lowest harmonic mean which is calculated from FRR and FAR. Next the suitable threshold, harmonic mean, FRR and FAR were got from a person and, the average FRR ($\overline{FRR}$) and the average FAR ($\overline{FAR}$) were calculated to appraise the overall performance of the system as follows.

$$\overline{FRR} = \frac{\sum_{i=1}^{N} FRR_i}{N} \tag{5}$$

and

$$\overline{FAR} = \frac{\sum_{i=1}^{N} FAR_i}{N} \tag{6}$$

where N is the total number of persons in the experiment, FRR_i and FAR_i are the FRR and the FAR belongs to person i, respectively.

For low-resolution face image verification, the harmonic mean, $\overline{FRR}, \overline{FAR}$ of each descriptor is shown in Table 2. It can be concluded that MPEG7-EHD is the appropriate descriptor for comparison between two images with different levels of resolution. The MPEG7-EHD will be used in the next part of this research.

Table 2 Comparison of The Five Descriptors in Term of The Average FRR and The Average FAR and Their Harmonic Mean (H).

Descriptor	$\overline{FRR}$	$\overline{FAR}$	H
Auto Correlograms	0.8000	0.1364	0.2331
Tamura's Texture	0.7818	0.1473	0.2479
Color Histogram	0.5455	0.1982	0.2907
MPEG7-EHD	**0.7091**	**0.1364**	**0.2287**
CEDD	0.5273	0.1927	0.2823

5.2. Research Part II Experiment and Results

For data collection process, samplings were random to guarantee variety of data. Table 3 showed general information of sample.

Table 3 General Information

Gender	Number
Male	97
Female	123
Age (years)	
18-24	24
25-40	104
> 41	92
Income (Baht)	
0 - 15,000	26
15,001 – 30,000	53
30,001 – 45,000	51
> 45,000	90
Education	
Under Bachelor Degree	18
Bachelor Degree	136
Master Degree	60
Higher than Master Degree	6

This research attempts to enhance authentication method of online transaction. The new proposed process was created and performance was assessed. Visual Basic .NET was used for programming the proposed process. In Part 2 of questionnaire, problem from traditional online banking systems were provided. All problems from this part were analyzed and leaded to requirement of the proposed process. The results in Table 4 showed the number of samples voting for each problem from traditional system.

Table 4 Problems from Traditional system

Problem leads to Requirement	**Number**
Signature is not well in investigated by merchant	161
Signature can be copied easily	134
SMS does not arrive within 1 minute	72
There are too many steps in traditional online internet banking process	45
Traditional internet banking verification process takes long time	60
Process remains on loading page and stop processing.	68

Note: each individual can answer more than one item

For accuracy of face matching verification process, threshold was calculated from samples using method that similar to Five-fold cross-validation. In this step, 100 persons were set as a dataset. This dataset was asked for two types of images to be kept as a sample: (1) low-resolution face image and (2) high-resolution face image with resolution of 3.0 megapixels. First, the dataset was split randomly into four mutually exclusive subsets equally. Four subsets were combined to the training set of 80 persons while the remaining subset is test set of 20 persons. From the five-fold cross validation, this manner repeats four times depending upon the subset chosen for the test set. Then, five training set gives the five thresholds based on steps of calculation in research part I for face verification process. After that, each threshold was used to evaluate the acceptance rate of the verification process on each test set as shown in Table 5. Finally, the average accuracy from five subsets was calculated as well.

Table 5 Thresholds and Accuracy of Five-Fold Cross Validation

	Threshold	**Accuracy (%)**
Data Set 1	139.784326	100
Data Set 2	139.446372	100
Data Set 3	127.496612	100
Data Set 4	132.803408	100
Data Set 5	138.812864	95
Average	135.668717	99

The results of the proposed process can be seen from comparison table. In this research, traditional process of online payment in Thailand was separated into two types: EDC and OTP. The proposed process was applied for both EDC and OTP processes. The simulation steps of online payment processes are depicted in comparison manner as shown Table 6 and Table 7.

Table 6 Traditional EDC Process Compared with the Proposed Process

	Traditional Process	**The Proposed Process**
Request authorization	Swipe card through magnetic card reader	Swipe card through magnetic card reader
Payment	Enter amount and confirm	Enter amount and confirm
Print pay in slip for merchant	Print slip for customer to verification process	-
Verification	Customer gives a signature	Face Matching Verification
Confirmation	Print sale slip for customer	Print sale slip for customer

Table 7 Traditional OTP Process Compared with the Proposed Process

	Traditional Process	**The Proposed Process**
Start process	Press payment button on the screen	Press payment button on the screen
Verification	Fill in card information	Fill in card information
	Request One Time Password	-
	Fill in One Time Password	Face Matching Verification
Request authorization	Click 'Submit' button	- (Auto request)
Confirmation	Redirect to Confirmation Page	Redirect to Confirmation Page

The questionnaire was created to keep the evaluation value based on hypotheses and objective of the research. 35 persons were selected randomly to be the sample set to test the proposed process for comparing with traditional process. After that the evaluation will be used for the analysis of the proposed process.

Hypotheses were set to answer:

H_0: Statistical means of traditional process and the proposed process are equal at 5% significance level.

H_1: Statistical means of traditional process and the proposed process are not equal at 5% significance level.

To analyze for the results, questionnaire was handed to participants before and after tested the proposed process. This section provides information about traditional process compared with the proposed process. Results from questionnaire can be explored from Table 8.

Table 8 Results before and after Using the Proposed Process.

Scale / Feature	1 (Not Satisfied)		2 (Less satisfied)		3 (Satisfied)		4 (More Satisfied)	
	Traditional (before)	Proposed process (After)	Traditional (before)	Proposed process (After)	Traditional (before)	Proposed process (After)	Traditional (before)	Proposed process (After)
Complexity	2	0	21	10	11	19	1	6
Learnability	4	0	18	1	13	25	0	9
Consistency	3	0	16	15	14	17	2	3
Operability	0	1	12	4	22	20	1	10
Reliability	1	1	15	6	15	15	4	13
Accuracy	4	0	9	13	16	16	6	6
Functionality	0	0	16	8	16	17	3	10
Trustworthiness	5	0	12	9	13	9	5	17
Efficiency	5	0	14	1	13	17	3	17
System Interface	3	0	6	0	0	21	26	14
Effectiveness	4	0	8	5	0	18	23	12
Privacy	1	0	19	13	0	15	15	7
Time of usage	7	0	10	3	0	16	18	16
Suitability	4	2	6	4	0	20	25	9

Chapter 6. Analysis and Discussion

The intention of this research is to compare MPEG7-EHD with reliable descriptors and use that method enhances the authentication method of online transactions. The result of authentication enhancement is evaluated by performance of the proposed system comparing with the traditional approach.

6.1. Research Part I Analysis

MPEG7-EHD is the best descriptor in term of harmonic mean calculated from the $\overline{FRR}$ and the $\overline{FAR}$. However, CEDD gives a good balance in both $\overline{FRR}$ and $\overline{FAR}$. Therefore, these two descriptors were chosen for further analysis. For each of descriptors, each image condition was independently considered with the $\overline{FRR}, \overline{FAR}$. and the result as harmonic mean as shown in Table 9 and Table 10.

Table 9 Comparison of the Five Image Conditions in Terms of the Average FRR and the Average of FAR and their Harmonic Mean (H) by Using MPEG7-EHD.

Image Condition	$\overline{FRR}$	$\overline{FAR}$	H
Regular face Image	0.0909	0.6909	0.1607
Overexposed face Image	**0.0909**	**0.5818**	**0.1572**
Underexposed face Image	0.7273	0.1000	0.1758
Non-Frontal Face Image	0.0909	0.7818	0.1627
Face image with facial expression	0.0909	0.8091	0.1635

Table 10 Comparison of the Five Image Conditions in Term of the Average FRR and the Average of FAR and their Harmonic Mean (H) by Using CEDD.

Image Condition	$\overline{FRR}$	$\overline{FAR}$	H
Regular face Image	0.8182	0.1091	0.1925
Overexposed face Image	0.0909	0.7727	0.1627
Underexposed face Image	0.6363	0.1727	0.2717
Non- Frontal Face Image	0.0909	0.7091	0.1612
Face image with facial expression	**0.7273**	**0.0636**	**0.1170**

The difficulty of this research is comparing two images with different levels of resolution or information. Five face images with conditions that could affect process during usage of credit card were considered. Moreover, face image kept in database should be low resolution image due to limitation of space. Since CEDD uses texture and color of image as information to compare, then CEDD is suitable for image with facial expression. Because of image with facial expression can provide various information in details of image. However, MPEG7-EHD used edge of image as main feature, and then this descriptor is better than the others. Even though low resolution image does not provide enough information, nevertheless, edge and margin of image still be sufficient to distinguish two images. Therefore, it can be assumed that MPEG7-EHD is the most suitable descriptor for comparing two images with different levels of resolution.

6.2. Research Part II Analysis and discussion

After all data was collected, it was analyzed by statistical analysis. The first part of the questionnaire will ask about general information of participants. This part of result can be used to analyze user behavior.

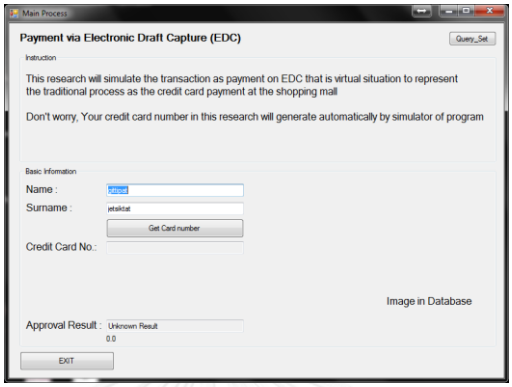
6.2.1. Proposed process

For the proposed process, requirement from user are needed to create a suitable program. Answers from Part 2 of the questionnaire were analyzed. The result showed that 100% of users have ever been used traditional process of online banking before. This can be assumed that participants have basic knowledge for all following questions.

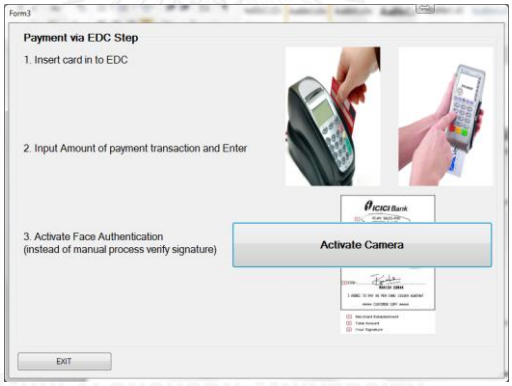
From Table 4, both technologies, EDC and OTP faces problem when processing online payment. It can be noticed that signature is not well investigated and can be copied easily. This important problem should be solved when creating the proposed process. The other problems are SMS not received, process transaction taking long time.

The proposed process was created. For accuracy of the proposed process, threshold value was set to judge similar faces. From Table 5 in Chapter 5, it

can be seen that the most suitable threshold value is 135.6687 with 99% accuracy. The simulation screen of proposed process with face matching verification can be separated into two process based on EDC and OTP process. For EDC the result was shown as Figure 21. And for OTP the result was shown as Figure 26.



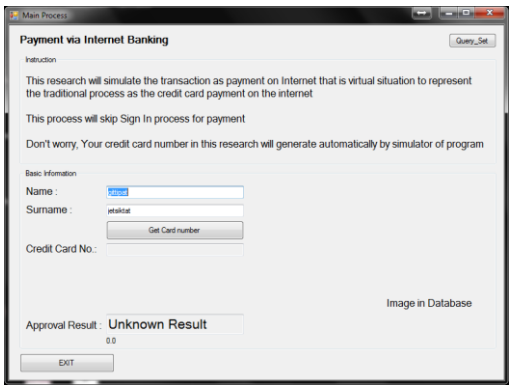
a.



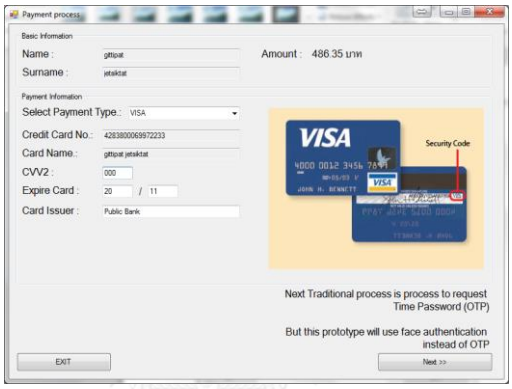
b.

C.

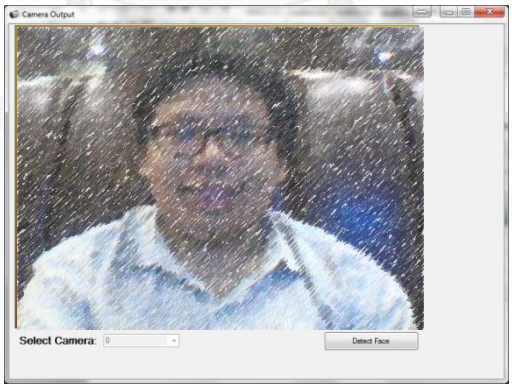
Figure 25. Simulation of Proposed Process Screen (via EDC)



a.



b.



c.

Figure 26. Simulation of Proposed Process Screen (via OTP)

6.2.2. **Result analysis**

The analysis of proposed process performance is shown as results below

Table 11 Paired Samples Statistics

			Mean	N	Std. Deviation	Std. Error of Mean
Usability	Complexity	Traditional process	2.31	35	0.631	0.107
		Proposed process	2.89	35	0.676	0.114
	Learnability	Traditional process	2.26	35	0.657	0.111
		Proposed process	3.23	35	0.490	0.083
	Consistency	Traditional process	2.43	35	0.739	0.125
		Proposed process	2.66	35	0.639	0.108
	Operability	Traditional process	2.69	35	0.530	0.090
		Proposed process	3.11	35	0.718	0.121
Capability	Reliability	Traditional process	2.63	35	0.731	0.124
		Proposed process	3.14	35	0.810	0.137
	Accuracy	Traditional process	2.69	35	0.900	0.152
		Proposed process	2.80	35	0.719	0.122
	Functionality	Traditional process	2.63	35	0.646	0.109
		Proposed process	3.06	35	0.725	0.123
	Trustworthiness	Traditional process	2.51	35	0.919	0.155
		Proposed process	3.23	35	0.843	0.143
	Efficiency	Traditional process	2.40	35	0.847	0.143
		Proposed process	3.46	35	0.561	0.095
Satisfaction	System Interface	Traditional process	3.40	35	1.063	0.180
		Proposed process	3.40	35	0.497	0.084
	Effectiveness	Traditional process	3.20	35	1.158	0.196
		Proposed process	3.20	35	0.677	0.114
	Privacy	Traditional process	2.83	35	1.043	0.176
		Proposed process	2.83	35	0.747	0.126
	Time of usage	Traditional process	2.83	35	1.272	0.215
		Proposed process	3.37	35	0.646	0.109
	Suitability	Traditional process	3.31	35	1.132	0.191
		Proposed process	3.03	35	0.785	0.133
Total		Traditional process	2.90	35	0.538	0.0910
		Proposed process	3.35	35	0.421	0.0727

Table 12 Paired Sample Tested

Comparing between traditional process and the proposed process	Paired Differences					t-score	df	Significant (2-tailed)
	Mean	Std. Deviation	Std. Error Mean	95% Confidence Interval of the Difference				
				Lower	Upper			
Complexity	-0.571	0.850	0.144	-0.863	-0.279	-3.977	34	0.000
Learnability	-0.971	0.891	0.151	-1.277	-0.665	-6.453	34	0.000
Consistency	-0.229	1.060	0.179	-0.593	0.135	-1.276	34	0.211
Operability	-0.429	0.778	0.131	-0.696	-0.161	-3.260	34	0.003
Reliability	-0.514	1.095	0.185	-0.890	-0.138	-2.779	34	0.009
Accuracy	-0.114	1.255	0.212	-0.545	0.317	-0.539	34	0.594
Functionality	-0.429	1.008	0.170	-0.775	-0.082	-2.514	34	0.017
Trustworthiness	-0.714	1.126	0.190	-1.101	-0.327	-3.751	34	0.001
Efficiency	-1.057	1.110	0.188	-1.438	-0.676	-5.635	34	0.000
System Interface	0.000	1.188	0.201	-0.408	0.408	0.000	34	1.000
Effectiveness	0.000	1.237	0.209	-0.425	0.425	0.000	34	1.000
Privacy	0.000	1.163	0.197	-0.400	0.400	0.000	34	1.000
Time of usage	-0.543	1.379	0.233	-1.017	-0.069	-2.328	34	0.026
Suitability	0.286	1.250	0.211	-0.144	0.715	1.352	34	0.185
TOTAL	-0.449	0.682	0.115	-0.683	-0.215	-3.895	34	0.000

Two hypotheses were proposed in Chapter 5.

To analyze both hypotheses, H_0 and H_1 from the T-Test, the result can be seen from statistical analysis

From Table 11 and Table 12, the overall result showed that T-Test score is -3.895 and Significant = 0.000. Then significance < 0.05 is sufficient evidence at significance level to reject the null hypothesis. It can be noticed that overall mean of traditional process different to and lower than that of proposed process.

To guarantee correctness of the result, there were specific detail support results in term of usability, capability and user satisfaction. These different features were analyzed in the following step. Statistical analysis details from

Table 12 showed that each feature has different statistical value. To support total result, each detail was analyzed separately using hypotheses and statistical analysis.

In term of Usability

Complexity of the process

Complexity can be described by means of interaction between entities. Numbers of steps to process transaction is important to evaluate complexity of the proposed process. For statistical analysis, null and alternative hypotheses were set:

H_0: Statistic mean of complexity from traditional process and proposed process are equal at 5% significance level.

H_1: Statistic mean of complexity from traditional process and proposed process are not equal at 5% significance level.

From Table 12, the result showed that T-Test score is -3.977 and Significance = 0.000. Then significance < 0.05 is sufficient evidence at significance level to reject the null hypothesis. From Table 11, it can be noticed that mean of complexity of the process are different to and lower than mean of the proposed process. Statistical mean of this feature in traditional process is 2.31. Conversely, the proposed process means is 2.89 which is higher.

This statistical analysis result was collaborating with reason that complexity of the system is step of payment process. If comparing traditional process with the proposed process, it can be noticed that proposed process has less number of steps of transaction than that of traditional system in both EDC and OTP transactions. From Table 6 and Table 7, it can be seen that steps of print pay in slip for merchant of EDC process and request One Time Password of OTP process have been reduced. Therefore, it can be assumed that complexity of proposed process is decreasing from traditional process.

Learnability of the process

Learnability can be understood by means of which the process is easy to learn and understand at the first time of usage. For statistical analysis, null and alternative hypotheses were set:

H_0: Mean of learnability from traditional process and proposed process are equal at 5% significance level.

H_1: Mean of learnability from traditional process and proposed process are not equal at 5% significance level.

From Table 12, the result showed that T-Test score is -6.453 and Significance = 0.000. Then significance < 0.05 is sufficient evidence at significance level to reject the null hypothesis. From Table 11, it can be noticed that mean of learnability of the process are different to and lower than mean of the proposed process. Statistical mean of this feature in traditional process is 2.26. Conversely, the proposed process mean is 3.23 which is higher.

This could be a result from the process that is easier to understand. Learnability of the process means that the process of proposed process is easy to understand by user at first time of use. Statistical mean from user stated that the proposed process is easier to learn than traditional process. This is supported by ability of all users to understand system and they can use system correctly by following the instruction. If system is easy to learn and understand, it can be noticed that system is not complicated.

Consistency of the process

Consistency of the process is related to the process with face matching verification compared with traditional process without face matching verification. For statistical analysis, null and alternative hypotheses were set:

H_0: Mean of consistency from traditional process and proposed process are equal at 5% significance level.

H_1: Mean of consistency from traditional process and proposed process are not equal at 5% significance level.

From Table 12, the result showed that T-Test score is -1.276 and Significance = 0.211. Then significance > 0.05 is sufficient evidence at significance level to accept the null hypothesis. From the result, it can be noticed that consistency of the proposed process is not different from traditional process. Statistical mean of consistency also presents result in the same way. Before and after using face matching verification, difference of means is 0.23. However, this number is slightly different and cannot be counted as significant number. Therefore, it can be noticed that consistency of the process is on the same level for both traditional process and proposed process.

This outcome was supported by reason that consistency can be seen from unitary of the process. A new module was well integrated with old system. There is no barrier in both traditional process and the proposed process with face matching. Payment system is still workable and end result remains the same. This reason brings the same result in traditional process and the proposed process.

Operability of the process

Operability was described in terms of smooth operating and no conflict when process transaction with face matching verification. For statistical analysis, null and alternative hypotheses were set:

H_0: Mean of operability from traditional process and proposed process are equal at 5% significance level.

H_1: Mean of operability from traditional process and proposed process are not equal at 5% significance level.

From Table 12, the result showed that T-Test score is -3.620 and Significance = 0.003. Then significance < 0.05 is sufficient evidence at significance level to reject the null hypothesis. From Table 11, statistical mean of this feature in traditional process is 2.69. Conversely, the proposed process means is 3.11 which is higher. It can be summed that face matching verification increases usability and helps process well operated with user.

As Operability of the process means system is smooth operating and no conflict when process transaction. After tested new proposed process with participants, all participants understood process and were able to processed transaction by themselves. This supports statistical analysis that the proposed process was operated better than traditional system.

In term of Capability

Reliability of the process

Reliability can be described by means of reliable of the process. The proposed process with face matching verification should be able to increase security to guarantee that process is more reliable than traditional process with signature or OTP. For statistical analysis, null and alternative hypotheses were set:

H_0: Mean of reliability from traditional process and proposed process are equal at 5% significance level.

H_1: Mean of reliability from traditional process and proposed process are not equal at 5% significance level.

From Table 12, the result showed that T-Test score is -2.779 and Significance = 0.009. Then significance < 0.05 is sufficient evidence at significance level to reject the null hypothesis. It can be assumed that reliability of the process before and after adding face matching verification was different. From Table 11, statistical means of this feature in traditional process is 2.63. Conversely, the proposed process means is 3.14 which are higher. In term of reliability, this proposed process uses faces matching for verification process. Because face is permanent and not easy to change, this provides more reliability for user when processed the transaction. Moreover, face cannot be stolen as PIN or easy to be copied as signature. This reason can strongly support statistical result that reliability of the proposed process is increased.

Accuracy of the process

Accuracy was defined as accurate of the process with face matching verification. However, perception of user focuses on accurate when

transactions proceeded. For statistical analysis, null and alternative hypotheses were set:

H_0: Mean of accuracy from traditional process and proposed process are equal at 5% significance level.

H_1: Mean of accuracy from traditional process and proposed process are not equal at 5% significance level.

From Table 12, the result showed that T-Test score is -0.539 and Significance = 0.594. Then significance > 0.05 is sufficient evidence at significance level to accept the null hypotheses. After analysis, in term of accuracy, statistical means are similar. For traditional process, statistical mean is 2.69 while statistical mean for the proposed process is 2.80. It can be noticed that value is slightly different.

The reason that participants scored accuracy from traditional process and the new proposed process could be explained by Table 6 and Table 7. Even though accuracy affects the quality or state of being correct and threshold result confirms 99% accuracy on face matching verification process. However, user can perceive accuracy only from confirmation of transaction. If transaction can be processed then accuracy of process is acceptable.

Functionality of the process

Functionality can be described by means of practical of the process. If compared proposed process to traditional process, the proposed process with face matching verification should be secure and practically to use in real system. For statistical analysis, null and alternative hypotheses were set:

H_0: Mean of functionality from traditional process and proposed process are equal at 5% significance level.

H_1: Mean of functionality from traditional process and proposed process are not equal at 5% significance level.

From Table 12, the result showed that T-Test score is -2.514 and Significance = 0.017. Then significance < 0.05 is sufficient evidence at significance level to reject the null hypothesis. From Table 11, statistical mean of this feature in traditional process is 2.63. Conversely, the proposed

process mean is 3.06 which is higher. It can be summed that face matching verification increases capability in term of function.

As function of traditional process is sign a signature when using EDC and request SMS (Short Message Service) in OTP. On the other hand, function of the proposed process is face matching verification. In comparing, in traditional process user has to spend more time to when sign a signature or request OTP. Participants are more comfortable with active camera function when verify faces than print slip function or request OTP function.

Trustworthiness of the process

Trustworthiness can be understood by means of which face matching verification process can increase security of payment process. For statistical analysis, null and alternative hypotheses were set:

H_0: Mean of trustworthiness from traditional process and proposed process are equal at 5% significance level.

H_1: Mean of trustworthiness from traditional process and proposed process are not equal at 5% significance level.

From Table 12, the result showed that T-Test score is -3.751, df = 34 and Significance = 0.001. Then significance < 0.05 is sufficient evidence at significance level to reject the null hypotheses. From Table 11, statistical mean of this feature in traditional process is 2.51. Conversely, the proposed process mean is 3.23 which is higher. It can be concluded that the proposed process with face matching verification is more trustworthiness than traditional process.

This statistical analysis result was collaborating with reason that security of online payment will be increased if added face matching verification into system. Face is a unique biometric that cannot be copied and unforgettable. Therefore, it would be more suitable than signature and PIN verification.

Efficiency of the process

Efficiency can be described as ability of verification process. Proposed process with face matching verification should be more efficient than traditional

process because face can provide more security to user. For statistical analysis, null and alternative hypotheses were set:

H_0: Mean of module efficiency from traditional process and proposed process are equal at 5% significance level.

H_1: Mean of module efficiency from traditional process and proposed process are not equal at 5% significance level.

From Table 12, the result showed that T-Test score is -5.635 and Significance = 0.000. Then significance < 0.05 is sufficient evidence at significance level to reject the null hypothesis. From Table 11, statistical mean of this feature in traditional process is 2.40. Conversely, the proposed process mean is 3.46 which is higher. It can be concluded that the proposed process with face matching verification is more efficient than traditional process.

Efficiency is an ability of verification process when process was finished. It can be noticed that face matching verification can provide more efficient to process in term of security because of many reasons. Face cannot be copied easily as signature. Also, face matching verification is more convenience than OTP. Users did not concern about security when they did not receive OTP or when changing phone number. These reasons support result that efficiency of the proposed process is increasing.

In term of User satisfaction

System Interface

System interface is interface of verification process when users proceed payment transaction. For statistical analysis, null and alternative hypotheses were set:

H_0: Mean of system interface from traditional process and proposed process are equal at 5% significance level.

H_1: Mean of system interface from traditional process and proposed process are not equal at 5% significance level.

From Table 12, the result showed that T-Test score is 0.000 and Sig = 1.000. Significance > 0.05 is sufficient evidence at significance level to accept

the null hypothesis. From statistical analysis, mean of traditional process is 3.40 as same as mean of the proposed process. It can be said that interactions between user and system are still the same. For the proposed process, even face matching verification process was added, however, the other processes such as verification, confirmation or payment process interface remain the same. Some participants cannot identify the difference because they still have to fill card information or press button as traditional process. Therefore, evaluation of this feature remains the same in both processes.

Effectiveness of the process

Effectiveness was described as effective of security when added face matching verification into payment process. For statistical analysis, null and alternative hypotheses were set:

H_0: Mean of module effectiveness from traditional process and proposed process are equal at 5% significance level.

H_1: Mean of module effectiveness from traditional process and proposed process are not equal at 5% significance level.

From Table 12, the result showed that T-Test score is 0.000 and Significance = 1.000. Significance < 0.05) is sufficient evidence at significance level to accept the null hypothesis. From the result, it can be noticed that consistency of the proposed process is not different from traditional process. Statistical mean of privacy also presents result in the same way. Before and after using face matching verification. From statistical analysis, mean of traditional process is 3.2 as same as mean of the proposed process.

There is no difference in statistical result because users do not feel the difference when processed transaction. Even though verification method is different and security is increased. Nevertheless, the proposed process still needs participation from user. Also, payment confirmation method is not different from traditional process. This causes user does not feel the effectiveness differently.

Privacy of the process

Privacy of the process was concerned when use face image is main information. Some may feel that verification process is not private and secure if face image of user was disclosed. For statistical analysis, null and alternative hypotheses were set:

H_0: Mean of privacy from traditional process and proposed process are equal at 5% significance level.

H_1: Mean of privacy from traditional process and proposed process are not equal at 5% significance level.

From Table 12, the result showed that T-Test score is 0.000 and Significance = 1.000. Significance < 0.05 is sufficient evidence at significance level to accept the null hypothesis. From the result, it can be noticed that consistency of the proposed process is not different from traditional process. Statistical mean of privacy also presents result in the same way, before and after using face matching verification. From statistical analysis, mean of traditional process is 2.83 as same as mean of the proposed process.

In order to proceed transaction, two image from user must be taken, the first image is a low-resolution image for database while the second image was taken when user proceeded payment step, On the other hand, for traditional process, user was asked for telephone number to kept on database as well. Both face image and telephone number are personal information that might be confidential for some user. This is the reason why analysis results of traditional process and new proposed process were almost the same.

Time of usage

Time of usage can be described by means of time to proceed payment process. For statistical analysis, null and alternative hypotheses were set:

H_0: Mean of time of usage from traditional process and proposed process are equal at 5% significance level.

H_1: Mean of time of usage from traditional process and proposed process are not equal at 5% significance level.

From Table 12, the result showed that T-Test score is -2.328 and Sig = 0.026 (Sig < 0.05) is sufficient evidence at significance level to reject the null hypothesis. From Table 11, statistical mean of this feature in traditional process is 2.83. Conversely, the proposed process mean is 3.37 which is higher.

Time of usage of the proposed process is less than that of traditional process. It can be assumed that after used face matching verification in the proposed process time that user processes transaction was decreased from traditional process. This statement was supported by Table 6 and Table 7 in chapter 5. It can be seen that when replaced verification process in traditional process with face matching, two steps of printing pay in slip for merchant of EDC and requesting One Time Password were reduced. If working steps were reduced, it clearly demonstrates that time will be decreased as well.

Suitability of the process

Suitability of process was concerned when used face image in verification process. This feature can be described as suitability of using face for verification method in public. For statistical analysis, null and alternative hypotheses were set:

H_0: Mean of module suitability from traditional process and proposed process are equal at 5% significance level.

H_1: Mean of module suitability from traditional process and proposed process are not equal at 5% significance level.

From Table 12, the result showed that T-Test score is 1.352 and Significance = 0.185. Significance < 0.05 is sufficient evidence at significance level to accept the null hypothesis. From Table 11, statistical means of this feature in traditional process is 3.31. Conversely, the proposed process means is 3.03 which is higher.

Suitability of the process was evaluated to find out user satisfaction. Some users concerned about using their face in public. This causes the result of suitability for the proposed process slightly decreased from used traditional process.

6.3. Conclusion

According to proof of hypotheses, statistical means from most of the features are increasing. However, some statistical means of features is equal between traditional process and the proposed process. The barrier and challenges have already been explained. Hence, it can be said that the proposed process has better performance and usability than the traditional processes.

Chapter 7. Conclusion and Future Research

7.1. Summary of research

This research provides three objectives to enhance security of online payment transaction based on credit card payment in Thailand. The findings of this research are shown as conclusion section below.

7.1.1. Research Objective 1

Research objective 1 was formulated in order to compare MPEG7-EHD with reliable descriptors which were generally used in the face similarity method under the different resolutions of two images. The difficulty of this task was comparing two images with different levels of resolution and information. From our experiment with five image descriptors and five conditions, it was indicated that MPEG7-EHD is the best descriptor because of using edge as the main feature. In other words, although the information of low resolution image is quite low, the edge gathered from the gradient of an image is still sufficient to be used to measure the difference between two images.

7.1.2. Research Objective 2

Research objective 2 was to enhance the authentication method of online transactions by creating the proposed process based on face matching verification method. In order to create proposed process, user suggested problem from traditional system. It can be noticed that there are many challenges that should be considered. The challenges are that security based on EDC process from signature is not well investigated and can be copied easily. It can be found that problems for OTP process are that SMS does not arrive within 1 minute and there are too many steps which take a long time.

When sample groups were asked about other problems, many obstacles were mentioned. There are barriers when using online payment when travelling abroad, SMS does not arrive. Moreover, process of changing phone

number is complicated. This problem leaded to requirement when created the proposed process.

The proposed process was created by following such requirement and able to solve security problem of traditional system. Also, the proposed process provided better solution for user when process online transaction.

7.1.3. Research Objective 3

Research objective 3 was aims to investigate performance of the proposed system comparing with the traditional approach. To achieve goal of research objective, questionnaires were set and have been reviewed by four experts. It was identified that there were several features to evaluate performance of the proposed process.

Key finding from this objective is that the proposed process is uncomplicated with higher system performance. Participants were asked to scale for usability, capability and user satisfaction in the questionnaire before and after using the proposed process. From result analyze and discussion, it can be noticed that the proposed process can increase system performance from traditional process. In term of usability, there is no barrier to increase performance when applied face matching verification into the system. Even though in term of the capability and user satisfaction can increase performance as well, nevertheless, there are some features that should be concern which are system interface, effectiveness and privacy. This is the challenge when created the proposed process. System interface remained the same when combine to the real system. The proposed process still needed participation from users as same as traditional process, this problem leads to the challenge when increased the effectiveness feature. Also, some participants concerned about privacy when handed face image data.

Despite some features should be concerned, the proposed process is still sufficient with security. In conclusion, enhance process of traditional system by created the proposed process is successfully with uncomplicated and higher performance.

7.2. Limitation of Research

As mentioned before, the research was about finding reliable descriptors which are used in the face similarity method and created proposed process with better performance. After studying through the research, there are many limitations in this study. For first objective, this research selects only five descriptors. This means other descriptors that have not been selected may be more suitable. However, that descriptor might not be generally used.

For objectives 2 and 3, if applied proposed process to the real system, size of sample set for calculating threshold value may be not large enough. Moreover, enhanced process has not be applied to real system. Hence, the statistical results from questionnaire may not precisely represent the real system of online banking based on credit card payment. Further, for more accuracy result, there should be more number of participants in this questionnaire..

7.3. Further Study/Research

For future research, other descriptors and conditions and more individuals should be also provided. Moreover, it is possible to develop the proposed process with higher performance using this research as a guide to continue. Researcher can use limitation of this research to develop for more accuracy result when created the proposed process. Furthermore, the proposed process is simulate of real system, then future research should be most similar as real system and continue developing by focusing on mobile platform to identify whether face matching verification can increase performance in online payment process based on credit card payment.

REFERENCES

[1] S. Phimoltares, "Artificial Neural Networks-Based Biometrics Technology" *University of the Thai Chamber Commerce Journal*, vol. 30, no. 1, pp. 90-103, January-March 2010.

[2] Y. D. Chun, N. C. Kim, and I. H. Jang, "Content-Based Image Retrieval Using Multiresolution Color and Texture Features," *IEEE Trans. Multimedia*, vol. 10, pp. 1073-1084, October 2008.

[3] J. Huang, S. R. Kumar, M. Mitra, W. Zhu, and R. Zabih, "Image Indexing Using Color Correlograms", in Proc. IEEE Computer Society Conf. Computer Vision and Pattern Recognition, pp. 762 – 768, 1997.

[4] T. Deselaers, D. Keysers, and H. Ney, "Features for Image Retrieval: An Experimental Comparison," Information Retrieval, vol.11, no. 2, pp. 77-107, 2008.

[5] R. Chakravarti, X. Meng, "A Study of Color Histogram Based Image Retrieval", in Proc. ITNG'09: 6th Int'l. Conf. Information Technology: New Generations, pp. 1323 – 1328, 2009.

[6] J. Hafner, H. S. Sawhney, W. Equitz, and M. Flickner, "Efficient Color Histogram Indexing for Quadratic Form Distance Functions", Journal of IEEE Transactions on Pattern Analysis and Machine Intelligence, vol.17, no. 7, pp. 729-736, 1995.

[7] S. A. Chatzichristofis and Y. S. Boutalis, "CEDD: Color and Edge Directivity Descriptor: A Compact Descriptor for Image Indexing and Retrieval", Computer Vision Systems, Lecture Notes in Computer Science, vol. 5008, pp. 312-322, 2008.

[8] T. Sikora, "The MPEG-7 Visual Standard for Content Description – An Overview", IEEE Transactions on Circuits and Systems for Video Technology, vol.11, no. 6, pp. 696-702, 2001.

[9] H. Tamura, S. Mori, and T. Yamawaki, “Textural Features Corresponding to Visual Perception”, IEEE Transactions on Systems, Man, and Cybernetics , vol. SMC-8, no. 6, pp. 460- 473, 1978.

[10] P. Howarth and S. Rüger, “Evaluation of Texture Features for Content-Based Image Retrieval”, Image and Video Retrieval, Lecture Notes in Computer Science, vol. 3115, pp. 326-334, 2004.

[11] C. Tanchotsrinon, S. Phimoltares, and S. Maneeroj, “Facial Expression Recognition Using Graph-Based Features and Artificial Neural Networks”, in Proc. IEEE Conf. Imaging Systems and Techniques, pp. 331- 334, 2011.

[12] S. J. Murdoch, S. Drimer, R. Anderson, and M. Bond, “Chip and PIN is Broken”, Proceedings of the IEEE Symposium on Security and Privacy, pp.433-446, 2010.

[13] H. O. Alanazi, R. Alnaqeib, A. K. Hmood, M. A. Zaidan, Y. Al-Nabhani., “On the Module of Internet Banking System”, *JOURNAL OF COMPUTING*, Vol. 2, pp.133-143, May 2010.

[14] M. O. Ali, “An internet banking system,” B.Sc. mini-thesis, Department of Computer Science., University of the western cape., Western Cape, South Africa, 2013.

[15] S. Chakravorti and T. To, “A theory of credit cards”, International Journal of Industrial Organization, Vol.25, No.3, pp. 583-595, June 2006.

[16] The UK Cards Association. (2012, April). *Credit cards: Your rights – a consumer guide* [Online]. Available: http://www.theukcardsassociation.org.uk/welcome/

[17] ConsumerFu. (2013, May). *Visa vs MasterCard vs American Express.* [Online]. Available: http://www.consumerfu.com/visa-vs-mastercard-vs-american-express

[18] *Card Acceptance Guidelines for Visa Merchants*, VISA Inc., USA, 2014.

[19] Q. Yang, Z. Cheng, and P. Song, “Research on Online Payment Mode Based On Internet Banking Payment Gateway”, Proceedings of the International Conference on Convergence Information Technology 2007, Oakland, USA, pp. 2038-2048, 2007.

[20] *How to help protect your business.* TD Merchant Services, Canada, 2012.

[21] T. P. Bhatla, V. Prabhu and A. Dua, “Understanding Credit Card Frauds”, TCS, Jun. 2013.

[22] MasterCard, (1994-2015). *How It Works: Secure Online Transactions & Payments.* [Online].Available:https://www.mastercard.com/mel/personal/en/cardholderservices/securecode/how_it_works.html

[23] M. V. Prakash, P. A. Infant and S. J. Shobana, “Eliminating Vulnerable Attacks Using One Time Password and PassText - Analytical Study of Blended Schema,” Proceedings of the International Conference on VLSI, Communications and Instrumentation, pp. 35-41, Nov. 2010.

[24] V. Matyas and Z. Riha, “Biometric Authentication – Security and usability,” IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security: Advanced Communications and Multimedia Security, Portoroz, 2002

[25] M. Yildiz and M. Gokturk, “Combining Biometric ID Cards and Online Credit Card Transactions,” Proceedings of the Fourth International Conference on Digital Society, St. Maarten, pp.20-24, 2010.

[26] L. C. Jain, U. Halici, I. Hayashi, S.B. Lee and S. Tsutsui, *Intelligent Biometric Techniques in Fingerprint and Face Recognition*, Florida: CRC Press, 1999.

[27] P. J. Phillips, R.M. McCabe and R. Chellappa, “Biometric Image Processing and Recognition,” The European Signal Processing Conference, 1998.

[28] A. K. Jain, A. Ross and S. Prabhakar, “An Introduction to Biometric Recognition,” *IEEE Trans. Circuits Syst. Video Technol,* vol. 14, no. 1, pp.1-29, Jan. 2014.

[29] R. Saini and N. Rana, "Comparison of various biometric methods," *International Journal of Advances in Science and Technology,* vol. 2, pp.24-30, Mar. 2014.

[30] L. Supriya, "IRIS Biometric For Person Identification," School of Information Technology IIT Kharagpur, west Bengal, india, Nov. 2012.

[31] V. R. E. Chirchi, L. M. Waghmare and E. R. Chirchi, "Iris Biometric Recognition for Person Identification in Security Systems," *International Journal of Computer Applications*, vol. 24, no. 9, pp.1-6, Jun. 2011.

[32] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain, "FVC2002: Fingerprint Verification Competition," *Proc. International Conference on Pattern Recognition (ICPR)*, pp. 744-747, Quebec City, Canada, Aug. 2002.

[33] S. Prabhakar, S. Pankanti and A.K. Jain, "Biometric Recognition: Security and Privacy Concerns" *IEEE COMPUTER SOCIETY*, Mar-April. 2003.

[34] W. Fan, H. Shu, E. Fife, and Q. Yan, "An Enhanced-security Fair E-payment Protocol," Proceedings of the 2009 WRI World Congress on Computer Science and Information Engineering, vol. 1, pp.516-519, Los Angeles, USA, March – April 2009.

[35] PBwork, (2010) "Advantages and Disadvantages of technologies," [Online]. Available:http://biometrics.pbworks.com/w/page/14811349/Advantages%20and%20disadvantages%20of%20technologies.

[36] P. J. Phillips, H. Wechsler, J. Huang and P. J. Rauss, "The FERET database and evaluation procedure for face-recognition algorithms" *Image and Vision Computing*, pp.295-306. 1998.

[37] H. Gravnas, "User's trust in Biometric Authentication Systems," M.S. thesis, Department of Computer Science and Media Technology, Gjovik University College, Stockholm, Sweden, 2005.

[38] G. Jetsiktat, S. Panthuwadeethorn, and S. Phimolthares, "A Comparison Study of Image Descriptors on Low-Resolution Face Image Verification," *In the Proc. of the 2014 Annual Summit and Conference on Asia-Pacific Signal and Information Processing Association*, pp.1-6, Siem Reap, December 2014.

[39] F. L. Podio "Personal Authentication Through Biometric Technologies," in, *IEEE 4th International Workshop on Networked Appliances.,* 2002, pp.57-66.

[40] D. Kumar and Y. S. Ryu, "A Brief Introduction of Biometrics and Fingerprint Payment Technology," in *IEEE 2nd International Conference on Future Generation Commun. and Networking Symposia*., 2008, pp.185-192.

[41] L. O'Gorman, "Seven issues with human authentication technologies," in *IEEE Workshop on Automatic Identification Advanced Technologies*, Tarrytown, NY, 2002, pp.185-186.

[42] Z. Z. Hosseini and E. Barkhordari, "Enhancement of security with the help of real time authentication and one time password in e-commerce transactions," in *IEEE 5th Conference on Information and Knowledge Technology.,* 2013, pp.268-273.

[43] W. S. Kim, B. Kang and Y. S. Chang, "A Credit card verification system by biometric method," in *IEEE 9th International Conference on Control, Automation, Robotics and Vision.,* 2006.

[44] S. A. Chatzichristofis, Y. S. Boutalis and M. Lux, "IMG(RUMMAGER): AN INTERACTIVE CONTENT BASED IMAGE RETRIEVAL SYSTEM.", in *IEEE 2nd International Conference on Similarity Search and Applications (SISAP), Computer Society*, Prague, Czech Republic, August 29-30, 2009, pp.151-153

[45] R. Kohavi, "A Study of Cross-Validation and Bootstrap for Accuracy Estimation and Model Selection", in *14th International Joint Conference on Artificial Intelligence(IJCAI).,* August 20, 1995, pp.1137-1143

[46] J. J. Hox and H. R. Boeije, "Data Collection, Primary vs. Secondary," in *Encyclopedia of Social Measurement*. New York: Elsevier, 2005, pp.593-599.

[47] C. Robson, Real World Research. A Resource for Social Scientists and Practitioner-Researchers. Oxford: Blackwell, 1993.

[48] Saunders, M., Lewis, P. & Thornhill, A. Research methods for business students (5th edition). UK: Prentice Hall. 2009

APPENDIX

Appendix A: Questionnaire

Questionnaire

Part 1 General Information

Gender O male O female

Age O 18-24 O 25-40 O >41

Income O <15,000 O 15,001-30,000

O 30,001-45,000 O >45,001

Education O Under Bachelor Degree O Bachelor Degree

O Master Degree O Higher than Master Degree

Part 2 Requirements

In order to enhance performance of new system, problem from traditional online banking system must be analyzed. Please give information and requirement for the new proposed process.

1. Have you ever used traditional online Internet banking process based on technologies below?

Electronic Data Capture (EDC)

O Yes O No (Please specify reason).....

One Time Password (OTP)

O Yes O No (Please specify reason).....

2. Do you think payment system will be better if biometric authentication was added?

O Yes O No

3. For EDC, please choose problems that occur when verifying a transaction?
(You can choose more than 1 choice)

O Signature is not well investigated by merchant.

O Signature can be copied easily.

O Other (Please specify).....

4. For OTP, please choose problems that occur when verifying a transaction? (You can choose more than 1 choice)

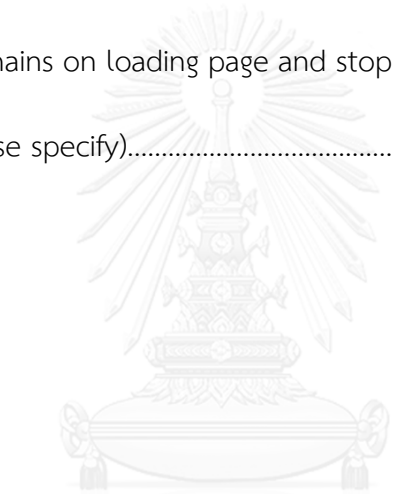
O SMS does not arrive within 1 minute.

O There are too many steps in traditional online internet banking process.

O Traditional internet banking verification process takes long time.

O Process remains on loading page and stop processing.

O Other (Please specify).....



Part 3 Evaluate traditional online internet banking process

On a 1-4 scale, how satisfied were you when using traditional online banking process?

	Before			
	1	2	3	4
Usability of the system				
Complexity				
Learnability				
Consistency				
Operability				
Performance of the system				
Reliability				
Accuracy				
Functionality				
Trustworthiness				
Efficiency				
User satisfaction				
System interface				
Effectiveness				
Privacy				
Time of usage				
Suitability				

Part 4 Evaluate Online Internet Banking process after applying face matching verification

On a 1-4 scale, how satisfied were you after using this proposed process?

	After			
	1	2	3	4
Usability of the system				
Complexity				
Learnability				
Consistency				
Operability				
Performance of the system				
Reliability				
Accuracy				
Functionality				
Trustworthiness				
Efficiency				
User satisfaction				
System interface				
Effectiveness				
Privacy				
Time of usage				
Suitability				

If you have additional suggestion please specify

VITA

Name: Gittipat Jetsiktat

Affiliation: Advanced Virtual and Intelligent Computing (AVIC) Center, Department of Mathematics and Computer Science, Faculty of Science, Chulalongkorn University.

Country: Thailand

Biography

1. Current Status/Position: I'm Gittipat Jetsiktat is a Master's degree student at the Department of Mathematics and Computer Science, Faculty of Science, Chulalongkorn University. I used to work with IBM, work for the Kasikornbank, THAILAND as Advance/Analyst programmers take role to develop business logic of ATM System. Currently, I'm work with DST Worldwide services Thailand Co., Ltd. as Analyst Programmer.

2. Education: I was graduated, Bachelor degree in Computer Sciences at Chulalongkorn University since 2011. Now I'm 2nd year student in Master's degree of Computer Science at Chulalongkorn University.

3. Research Interests: Gittipat interest the Image Recognition System and Security System with Biometrics informations.