ISSN:2320-0790

An International Journal of Advanced Computer Technology

# Security Enhancement for Online Signature Template on Mobile Devices Using Partial Hadamard Transformation

YATINDER KUMAR

*Abstract*— during our whole study we analyze that security is the main issue in Mcommerce and there are various methods by using which we can enhance the security. We learned that authentication plays an important role in security and we also learned that biometric authentication is the best way to authentication due to its uniqueness. So the security of biometric template is much more important because if anyone compromise with it then we loss it forever. In This paper we define a non invertible partial hadamard transformation which we have used to enhance the security of online signature verification process. The proposed methodology which we have used enhances the security and maintains the accuracy of the system. And we achieved two main things Diversity and revocability which are security factor used in security enhancement. So the security of biometric template is much more important because if anyone compromise with it then we loss it forever. There are mainly two important methods by which we can provide security to biometric template. These are biometric cryptosystem and cancellable metrics (transformation). The main advantage of partial hadamard is low computational cost because instead of multiplication it uses addition and subtraction. The main purpose is to enhance the security of online signature template by making it non invertible so that no one can compromise it.

*Keywords—mcommerce,biometric,mcommercesecurity hadamard transformation.*

## I. Introduction

First we are going to discuss some basic term which we have used while testing the security of Mcommerce. So what is testing? Testing is the process of checking the functionality and behavior of an application whether it is correct or not. In actual we perform testing in our daily life also while purchasing item we check whether the item is good (correct) or not. This one is the simplest definition of testing. We will discuss in detail later. Now we are going to discuss about the main concept. What is security testing? In technical term security testing is the process to check that whether a application is secured or not. If it is secured then up to which limit it is secured? Now we are going to discuss the main topic Mcommerce. As we now the today time is technology time and new-2 technologies are coming day by day Mcommerce is one of them. At present mobile phones are replaced by smart phones. So Mcommerce is the process of performing transaction on mobile phone which includes online shopping, banking transaction, bill payment, ticket booking, recharge etc. while we perform above all operation on mobiles then this operation is known as Mcommerce. Our main purpose is to check how much secure a Mcommerce application is? Which we discuss later .Now we discuss some basic term from which Mcommerce is arises i.e. Ecommerce also known as electronic commerce and also discuss why it is replaced by Mcommerce. Ecommerce is process of performing online transaction on desktop, laptops etc. which involve banking transaction, online shopping, and online ticket booking etc. now we discuss why ecommerce is replaced by Mcommerce. As we now it is not possible to carry desktops and laptops everywhere so that's why ecommerce is replaced by Mcommerce because mobile phones are portable and easy to carry and easy to use so they totally replaced ecommerce. But as we know if a thing has some advantages then it had some disadvantages also. The main challenge to Mcommerce is security. Mobile devices are not much secured as compare to desktop. So the main challenge in Mcommerce is that how to make a Mcommerce application secured. Security is the main issue in mobile commerce application. Now we discuss in detail what are the application, scope and security architecture of Mcommerce

### *1.1 Mcommerce*

Mcommerce is the process of performing online transaction using mobile phone like purchasing, selling of any item. It also include online banking, money transferring, online shopping, online ticket booking etc. so we can say Mcommerce are same as

ecommerce but the difference is that in ecommerce we uses a computer and in Mcommerce we uses a mobile devices and due to portability and accessibility mobile phones are widely in use and people are using mobile phones to perform various type of online transaction.

*1.2 Difference between M commerce and E commerce:*

1. Basic definition:-In m commerce transaction are done on mobile devices but in case of e commerce transaction are performed over computer.

2. Portable: - mobile devices are small in size and easy to carry but computer are large in size and not portable.

3. Accessibility: - we can access mobile phones from anywhere and from anyplace but in case of e commerce the action is performed from computer whose accessibility is limited due to a large no of reasons.

4. Security: - security is the main concern of Mcommerce. Mcommerce is less secure as compare to E commerce due to lots of factor.

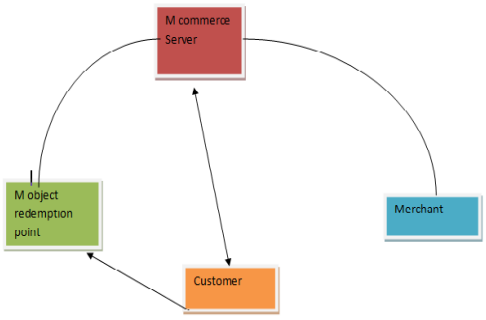
5. Speed: - Speed of E commerce is much more than m commerce because we use ecommerce which is connected through wires to a high speed broadband connection.

6. Cost: - cost is high for E commerce system as compare to m commerce devices.

*1.3 Mcommerce Architecture*

It contains four main parts:

1. M commerce server
2. Customer
3. Merchant
4. Redemption point




*1.4 Mobile threats*

There are mainly four types of threats to the mobile.

1. Application based threat
2. Web based threat
3. Network based threat
4. Physical threat

1. *Application based threat:-*

a) Malware: - is one that performs action without the knowledge of user. It changes some setting stop an running application, install a new application without the knowledge of user.

b) Spyware: - as the name suggests spy it steals the information, data from the user device without the user approval or knowledge.

c) Repacking: - in this type of attack the attacker pick any mostly used application and repack then by doing some changes to it and then put it again in the market to got access data of other users.

2. *Web based attack :-*

a) Phishing: - mostly used attack in phishing the attacker creates a duplicate interface to get access user login information. E.g. attacker creates a duplicate page for face book and out it in internet when user click on that link then duplicate interface opens and user puts his login details now attacker can easily got user login detail for performing action.

b) Driven by download: - in this type of attack when we visit some website than some application start downloading automatically so that it can be store on user pc and can get detail this type of attack is known as driven by download.

## II. LITERATURE SURVEY

**Anil K jain [1]** publishes a paper on "An introduction to biometric Recognition" in this paper we studied about different techniques of biometric system, types of error occurs in biometric system such as sensor noise, dry finger, changes in user physiological or behavioral characteristics. Advantages of the biometric system and disadvantages of the biometric system and what are various application of the biometric system and ease and security of the biometric system we studied different techniques used for biometric authentication and we also studied about the security of biometric system.

**Rashad Yazdanifard [2]** publishes a paper on "Mobile commerce and related mobile security issues". This paper presents what is m commerce?

Benefits of Mcommerce types of security issue in terms of security and also provide the solution by using which we can minimize the security issue. It is concerned with the various challenges that makes mobile commerce technology unsecured in the form of that any attacker can easily attack the confidential data transfer between the users and the merchant and also discussed the main advantages of Mcommerce

**Ioannis Kounelis, Gianmarco Baldini [3]** publish a paper on "An Architecture for secure Mcommerce application "in this paper we studied about architecture for Mcommerce. Author represent a secure Mcommerce architecture and also define the element of architecture interrelated with each other and how they are working. The role of the merchant, customer, Mcommerce server and the redemption point. We learn about secure architecture and security means. We learn about the way in which authentication is provided for the customer and the merchant. We also learned who actually transfer item to the customer.

**Jian Xu , TieJun Pan [4]** publish **a** paper on "Design and implementation of high security mobile payment system". as we know security is the main issue in Mcommerce and designing a secure system is also a challenge from this paper we come to know about how to design and implement a high security system for Mcommerce payment because during payment the whole data should me in a secure environment so that no one can attack them and we learned the different types of payment method in Mcommerce and how they can be perform action. We learned that secure system is more important when we concern about mobile payment system.

**Scarlet Schwiderski-Grosche [5] publish** a paper on "Secure Mcommerce" in this paper he discussed Mcommerce mean and its security challenges. We learned about the main security challenges such as authentication, authorization, integrity, confidentiality and come to know what are the importance of their properties without these properties we can't provide security to a Mcommerce application difference between Mcommerce and ecommerce and also the disadvantages of Mcommerce. We learned security challenges in term of network .Different type of mobile payment system.

**Sukjit Kaur, Anuj Kumar Gupta [6]** publishes a paper on "An efficient Authentication and payment method for Mcommerce" we learned the actual meaning of authentication and its importance in security. We learned how to authenticate a mobile user as we know during mobile payment it is very necessary to authenticate a user to prevent loss of data It is necessary to authenticate user before accessing the system. Method for authentication should be efficient so that no one can get easily attack it we learn how we can develop an efficient system for authentication and for payment.

**K.Shanmugam , Dr B.Vanathi [7]** publish a paper on " Enhancing secure transaction and identity authentication in Mcommerce " we learn about Mcommerce transaction, how transaction are performed and why security is important while performing mobile transaction, requirement for Mcommerce, different types of technique and algorithm used in transaction to improve the security and authentication process, we learned about barcode, biometrics, one time password and also learn the concept of fuzzy logic . How it works, when to use it and also we learned about the double encryption model.

**Wencheng Yang, Jucheng Yang [8] publish** a paper on "Biometrics for securing mobile payment: benefits, challenges and solution" we learned how biometric system works also learn that biometric authentication is the best method for authenticate a user due to its uniqueness. We learned biometric authentication can help in mobile payment. But there are some challenges in biometric also then also attacked by attackers so security is also an important issue in biometric system what are the challenges of using biometric in mobile payment and solve these problems.

**Arunkumar Gangula, Saad Ansari [9]** conducted a survey on "Survey on mobile computing security". in this paper author take a survey on mobile security .in this paper we learned about different types of attacks that are harmful to our mobile system there are various type of attack which are based on application based threat which include malware and spyware, web based attack which include phishing, auto download and then network based attack which include Wi-Fi sniffing, fire sheep type of attack and at last we learn about physical threat to mobile are lost or stolen of devices.

**A.K.M Harun-Ar-Rashid [10]** publish a paper on "Independent channel multi method multi factor authentication model for B2P remote commerce" in this paper we learned than a strong type of authentication is required for improve security and author discussed the multi factor authentication model. We learn that we can use more than one factor for authentication to improve security. In multi factor authentication method first we authenticate user based on personal identification number after that we use another method for example we can use biometric authentication. The important thing that we learned is that by applying more than one authentication method we can improve the security

**Rathgeb, Christian, and Andreas Uhl [11]** publishes a paper on "A novel approach for securing

biometric Template" in this paper we studied about biometric template protection and biometric cryptosystem and invisible watermarking technique for securing a biometric system, properties of a biometric system author defines how we can secure a template using a invisible watermarking techniques and also defines there are various techniques by which we can secure a biometric template. We studied if biometric template is compromised the it looses permanently because for example of fingerprint template is compromised then we can't generate different fingerprint sample because fingerprint are unique in nature.

**Napa Sae-Base [12]** publishes a paper on "Online signature on mobile device" in this paper we studied about online and offline signature securing a signature by using histogram technique it involves feature vector generation pre-processing and the quantization process which make a signature template secure we also studied how we can extract feature from a online signature by using it's x ,y coordinates, pressure, orientation and speed and also define online signature is best as compare to the offline signature due to security the histogram technique which the author is used is also a non invertible technique that define the signature template which we create can't be invertible if compromised.

**Song Way[13]** publishes a paper on "A hadamard Transform Based method for the design of cancellable fingerprint template" in this paper we studied about cancellable biometric and we studied the cancellable biometric provides non invertibilty, diversity and security in the system. We also studied about hadamard transformation hadamard is a transformation technique used in various field such as image processing etc. in hadamard we create matrix in the power of 2 but the author used the partial hadamard instead of hadamard the advantage of partial hadamard is that it is noninvertible and provides the accuracy and computation cost is also very less.

## III. PROPOSED METHODOLOGY

**Pre-processing**

In online signature process the first user perform signature on a mobile device than feature from that signature are extracted Online signature pre-processing is required to remove the dissimilarities presented at the instant the signature was taken from the user. These dissimilarities may be due to the lower resolution of the digital device which is used to obtain the signature of a person. These may be due to the reason if the genuine signatures of the person are taken in different situations that are in dynamic or static conditions.

**Feature Extraction**

In feature extraction process the various features of the signature such as its x, y coordinates, pressure, speed, orientation etc than we create a feature vector from the extracted features and after that creates histogram from that feature vector and after that we create function vector or feature vector from the histogram and at last we combine or concatenate all the feature vector to make a template. Extracting feature is a very important step in online verification of the signature. The feature extraction process starts by changing the time-domain data of a signature into a sequence of Cartesian vectors and attributes, as well as their derivatives. After this, each vector is also converted to a vector in the polar coordinate system.

**Template Generation**

Template creation is the most important part of the all process in template creation process all the features vector are concatenated to make a template and after that for securing that template we apply hadamard transformation on that template to make it non invertible so that if the template is compromised than no one can generate the original template from that compromised template A user template is created during the enrolment process where several signatures are acquired from a user and a feature set is calculated from each of the samples. A pair ($Q^u$ , $F^u$) including the step size vector and its accompanying feature vector template is then stored and later used to verify a query signature of the user u.

$$q^u(i) = \beta\sqrt{\left(\frac{1}{S}\right)\left(\sum_{j=1}^{S} f^{Sj}\,(i) - \mu_{f(i)}(u)\right)}\ , \quad i = 1, \dots, M$$

$$\mu_{f(i)}(u) = \left(\frac{1}{S}\right)\sum_{j=1}^{S} f^{Sj}\,(i) \quad i = 1, \dots, M$$

**Applying hadamard transformation**

When the template is generated than to make it more secure we applied hadamard transformation on it. Hadamard is invertible so we used partial hadamard transformation when we used partial hadamard than after multiplication with template a matrix of non square created and we know according to law of matrix the inverse of a non secure matrix does not exist. So the now the template we have created is a non invertible template.

**Secure Signature Template creation with using Partial Hadamard Transform**

However, a full-order Hadamard matrix is reversible; a sub matrix is formed or created by randomly selecting a subset of rows from full-order Hadamard matrix, which is non-invertible due to its non square in nature. We explain the partial Hadamard matrix

which we have selected according to our matrix which we have created from histogram techniques
Let $H_N$ denotes partial technique Hadamard matrix, which is created by selecting $S$ ($S$=244 in this case) rows of an $N\times N$ full-order Hadamard matrix $H_N$ so the matrix we have created is of $H_{244*256}$, and therefore the partial Hadamard matrix $H_N$ is non invertible. Now, apply following transformation to creating the template $T$:

$$T_{1*244} * H_{244*256} = X_{1*256}$$

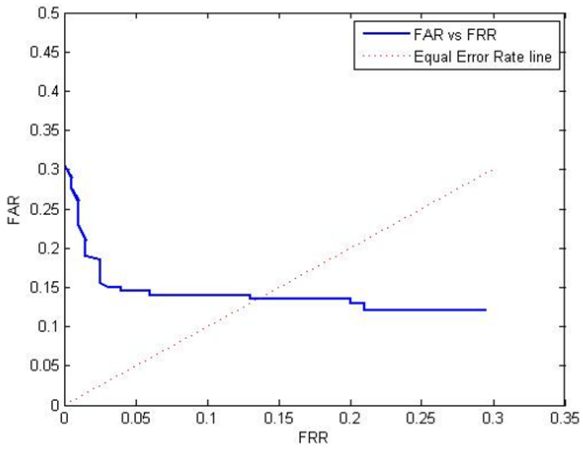
Where T is template which we have created from the histogram technique and 244 is the no of total bin we have used and due to this we make a matrix of 1*244. H is the partial hadamard which we have used. Why we used a hadamard of 244 instead of 256 the reason is that according to the law of matrix we can't multiply two matrixes until the column of first matrix is not equal to the row of the second matrix due to this we used partial hadamard of 244*256. After multiplying both the matrix we generated a new matrix or a secure template who is non invertible in nature. The reason behind is that if we try to calculate the inverse of the matrix than inverse does not exist because according to law of matrix the inverse of a non square matrix does not exist. Which proves that it is a non invertible matrix? Generally, Hadamard matrices are called geometrically, it means every two distinct rows in Hadamard matrix display two perpendicular vectors, where the combinatorial terms show which every two distinct rows contains matching entries in correctly half of the columns and unmatched entries in remaining columns. Conversely a Hadamard matrix. Hadamard matrices are reduced to cost of computation because instead of multiplication it uses the subtraction and addition of the operations. This lets the use of easier hardware to compute the transform or improve the speed of retraining because of less complexity.

**Signature verification**

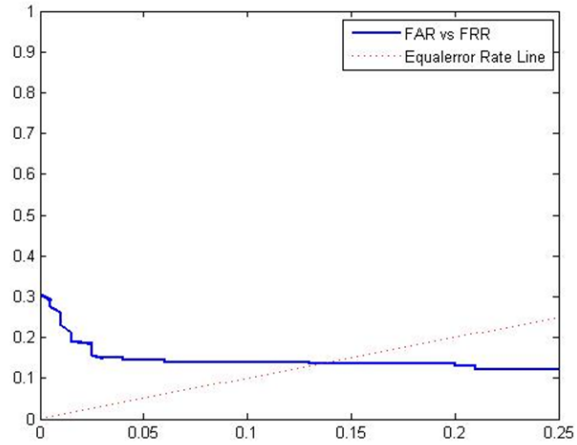
In the process of verification when the user gives the input, this input signature is to be verified by matching with the stored reference signal. The process of matching can be done by evaluating the Manhattan distance which is used in the current online signature verification system. If the variance between the test signature and the reference signature is less than the threshold value then signature will be taken as genuine but if the difference between the two is more than the predefined threshold then the test signature will be taken as fake. During verification, given that $t$ is said to be an online signature sample from user $u$, $\hat{F}^{(t|u)}$ is calculated using $Q^u$. Then the system derives a difference score using Manhattan distance between as,

$$Score = \sum_{i=1}^{M} |\hat{F}^{(t|u)} - \ddot{f}^{u}(i)|$$

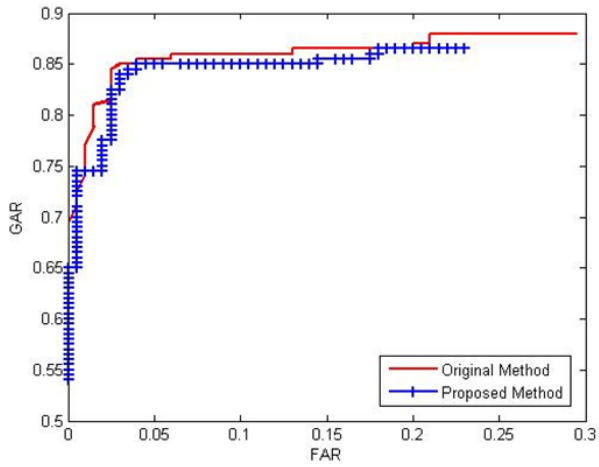
## IV. RESULTS




Proposed Method




Original Method




Comparison of the two methods

The results presented here, show that the GAR has still been maintained as the variation in the the values is very less as compared to the previous method. But due to the inclusion of partial Hadamard matrix, the security of the system is increased. This is because the applied partial Hadamard matrix transforms the template into non-invertible domain. This also adds up to the diversity and revocability as many number of templates can be generated using the different combination of the partial hadamard matrix. And hence the security also gets increased for the template as well as the biometric system.

## V. CONCLUSION

By the help of results, we can conclude that the proposed method enhances the security of the system to a great extent thereby improving the system and also maintaining the accuracy of the system as the GAR for the proposed system is not much different from that of the earlier system. The future work can be dealt in the area to further improve the accuracy so as to decrease the cases of false acceptance. The main advantage of applying partial hadamard is that we can also revoke a template if a template is compromise because we have $H_{244*256}$ *partial hadamard we can make template by shuffling rows and columns i.e we have 244! And 256! Ways to shuffle rows and columns so the another factor which we achieved is the revocability*

## REFERENCES


[1] Napa Sae-Bae(2014) "Online signature on Mobile device" IEEE Transaction on information forensics and security, vol. 9, no. 6, June 2014.

[2] Song Wang(2013)," A Hadamard Transform-Based Method for the Design of cancellable fingerprint template" 2013 6th International Congress on Image and Signal Processing (CISP 2013).

[3] K.P Tripathi(2011)," A Comparative Study of Biometric Technologies with reference human interface" International Journal of Computer Applications (0975 – 8887)Volume 14 No.5, January 2011.

[4] Anil K jain(2008),"Biometric Template Security" To appear in EURASIP Journal on Advances in Signal Processing, Special Issue on Biometrics,January2008.

[5] Rashad Yazdanifard (2011**)** "Mobile commerce and related mobile security issues" *International Conference on Software and Computer Applications IPCSIT vol.9 (2011) © (2011) IACSIT Press,Singapore*.

[6] Ioannis Kounelis, Gianmarco Baldini(2013), "An Architecture for secure Mcommerce application" 19th International Conference on Control Systems and Computer Science(2013).

[7] Jian Xu , TieJun Pan (2012), "Design and implementation of high security mobile payment system" International Conference on Communication Systems and Network Technologies(2012).

[8] Scarlet Schwiderski-Grosche, "Secure Mcommerce" Information Security group, Royal Holloway University of London Egham TW20 0EX UK.

[9] Sukjit Kaur, Anuj Kumar Gupta (2012) **"**An efficient Authentication and payment method for Mcommerce International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 4, June – 2012 ISSN: 2278-0181.

[10] Wencheng Yang, Jucheng Yang (2013), "Biometrics for securing mobile payment: benefits, challenges and solution" Image and signal Processing (CISP), 2013 6th International Congress (Volume:03).

[11] Nirav Jobanputra , Vijayendra Kulkarni publish a paper on " Emerging Security Technologies for mobile user accesses".

[12] K.Shanmugam , Dr B.Vanathi (2014) publish a paper on " Enhancing secure transaction and identity authentication in Mcommerce" Volume 2 | Issue NCETSE Conference | March 2014.

[13] A.K.M Harun-Ar-Rashid (2006) "Independent channel multi method multi factor authentication model for B2P remote commerce" Enterprise Distributed object computing Conference workshop,2006 EDOCW'06, 10th IEEE international.

[14] Christian Rathgeb " A Survey on biometric cryptosystem and cancellable biometric" l EURASIP Journal on Information Security 2011.

[15] Arun kumar Gangula, Saad Ansari (2013) "Survey on mobile computing security" in Proc. EMS, 2013, pp.536-542.

[16] Donato Impedovo(2008) "Automatic Signature verification" IEEE Transactions on systems, Man and cybernetics—part c: applications and reviews, vol. 38, NO. 5, September 2008.