A Novel Approach for Secure ATM Transactions using Fingerprint Watermarking

R.Angelinjosphia [1], Ms.PVS.Gayathri [2]
[1]PG Student, [2]Assistant Professor, Department of CSE, Chettinad College of Eng. and Tech, Karur

Abstract—This paper presents a technique for storing encrypted numeric data in fingerprint images through watermarking techniques. The four fingerprint images, where each image is further divided into 4 quadrants and each quadrant image is watermarked with the encrypted numeric digit. As the four fingerprints is watermarked with an altered ATM pin number of the same user, the proposed work finds application in security implementations based on cryptographic fingerprint watermarking. Such a combination of encryption and watermarking techniques provides a level of security and further protects the identity of the user from attacks due to the robustness of the technique. The experimental study is done on a limited number of users and the results show that our hybrid approach gives improved results in terms of other existing approaches in the literature.

Keywords *—Finger Watermarking, Finger Quadrants, ATM Transactions*

1. INTRODUCTION

In recent advancements in computer technologies offer many facilities for duplication, distribution, creation, and manipulation of digital contents. Encryption is useful for transmission but does not provide a way to examine the original data in its protected form. Cryptographic techniques are to provide matching in encrypted domains (like homomorphic encryption schemes), aliveness detection strategies, or other means of protecting the integrity of the entire authentication mechanism. Watermarking (WM) has been suggested as a means to resolve some of these problems as well and can potentially add additional functionalities to biometric systems.

The aim of watermarking is not to improve any biometric system, but to employ biometric templates as message to be embedded in classical robust watermarking applications like copyright protection in order to enable biometric recognition after the extraction of the WM. There are four types of watermarking process, they are

1. Embedding stage contains two domains in which Spatial domain is used for flipping the low-order bit of each pixels.

The Frequency domain does embedding the watermark in mid-frequency components which is relatively robust to noise, image processing and compression. The quality of the host image will be distorted significantly if too much data is embedded.

2. In Distribution stage Compression, transmission error and common image processing are seen as an attack on the embedded information

3. In Extraction stage, Blind is done by extracting without original image. Semi-blind is to rely on some data or features and Non-blind need original image.

4. In Detection stage it evaluates the similarity between the original and detected watermark. In False positive watermark is detected although there is none and in false negative no watermark is detected while there is one.

Fingerprinting is to trace the source of illegal copies. Different watermarks are embedded by the owner in the copies of the data that are supplied to different customers.

Authentication and data integrity which is used for verifying watermarks that are required to befragile that any modification to the image will destroy the mark.Copy Protection is the requirements for robustness against removal, ability of blind detection, capability of conveying non-trivial number of bits.

2. RELATED WORKS

AfzelNooree*t al.* [2] proposed a contextual fingerprint image for watermarking algorithm. The results of the proposed watermarked fingerprint and the extracted images are resilient to common attacks such as compression, filtering, and noise. The absence of watermarks or visual distortions in the extracted watermarks would reveal that the integrity of the fingerprint image has

been compromised. Farid Ahmed *et al*. [4]. It extends the digital watermarking technique Phase mark, developed for image authentication, to biometrics to assist in forensic analysis. As a result the need is to Bilge *et al.* [3] introduces two spatial be done to make it more robust so that it will work methods to embed watermark data into fingerprint images. Both methods do the encoding and decoding process. They propose to preserve fingerprint feature regions either by isolating singular point regions during watermarks embedding or adjusting the watermark embedding strength in order to guarantee that gradient directions remain within the analytically computed intervals. Gang Qu*et al.* [7] introduces a new methodology of fingerprinting for the purpose of IP protection. Finger print technique is used to well with non-trained fingerprints as well.

Abdel et al. [5], classify different techniques used for watermarking IP designs. They introduced a set of evaluation criteria then surveyed the current State-of-the-art in IP digital watermarking, and finally compared the different techniques available. Jana*et al*. [8] present a technology for combining a collusion-secure fingerprinting scheme based on finite geometries and a watermarking mechanism with special marking points for digital images.

3. PROPOSED SYSTEM

Khalil *et al*. [1] introduced a new technique called multi-resolution wavelet based digital watermarking method to hide the fingerprint minutiae data in fingerprint images. It requires the original image to extract the embedded minutiae. As a result this method is highly robust to compression and additive noise and to make the method more robust for attacks.Augot*et al*. [6] proposes the terms of watermarking, fingerprinting and monitoring and concludes that a trusted third party is needed to establish a verification service of watermarks. Using the DHWM scheme, this small amount of information is turned into copyright protection system, using a Trusted Third Party. reliability, security plays a key role. Even though many security and key management policies (e.g. Online pin validation, off line pin validation, Key management) where enhanced in the existing system, we are still prey to some level of vulnerabilities in ATM transactions.

For effective transactions we need some novel methods to handle. Many new methods were available for the integration of security. For a proper integration we need some key parameters to be combined together that enhances the integrity and the originality of the transactions to the maximum extent.

Apart from conventional transactions the integrity of transactions along with security is necessary. In case of ATM the primary and common way for security is its pin number. But pin number alone will not provide enough security. We need some constraining method to make sure that the pin number is well balanced for the user andprovider but not for the third party or hackers. With some integrated security policies we can make it effective for some potentialimprovement in ATM transactions. For integration we need some different security policies to be merged. preliminary stage in our system is formation of patterns through fingerprints with focus on formation of array locations for the pin number. Next, we will segment the captured fingerprints into 16quadrants. Each and every newly generated key or pin number will take its positions in the newly formed fingerprint pattern. Thereby we can also provide more authenticated service by including various fingerprint parameters for the security purposes.

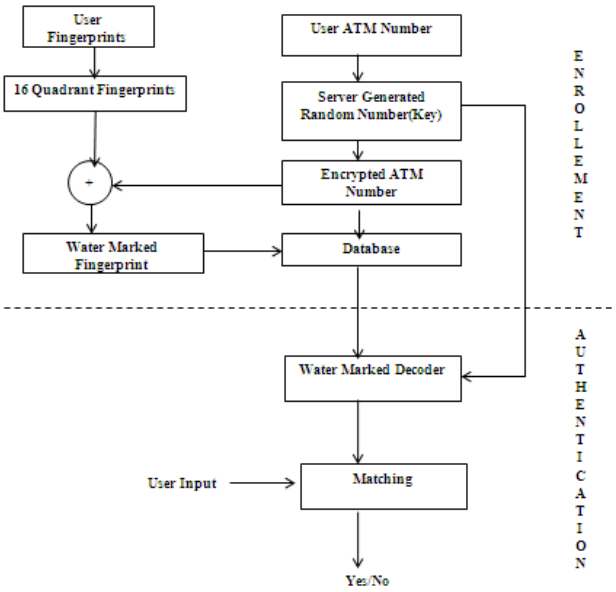

Fig.No 1. Architecture diagram

In proposed system, we aim to achieve a high sense of security for ATM transactions with the help of fingerprint watermarking and cryptographic concepts. The integration of these two methods helps to make the transactions more secure and reliable as per our expectation. In this proposed method, we combine two security features to enhance the collective function of transactions along with high confidential policies. Watermarking is one of the highly influenced methods for typically identifying ownership of the individual. After that we are marking the pin number on to the fingerprint pattern that we generated in the initial stage. Then the actual ATM key will reform into a new identity. So that misuse of pin number can be highly protected. Fig.No.1 represents the complete architecture of our proposed system.

FINGERPRINT PATTERN GENERATION:

As in Fig.No.2 user's fingerprints will be captured through the fingerprint scanner. The most Even though we are applying various constraints towards forming a secured pin number the user should be least aware of the processing going behind. As like a conventional transaction here also we using a normal ATM pin number of the card holder as its input. Each and every time the user enters his/her ATM key it will take a new form that is unknown to even the card holder. With the help of such a new key will enhance high level of security for the authenticated users.

Fig.No.2. Fingerprint scanner

USER INPUT:

USER PIN:

2	3	4	5

Fig.No.3. ATM Number

RANDOM NUMBER GENERATION AT THE SERVER:

Here we have logic for generating a new key for the corresponding user input. Fig.No.4 shows one of the server generated dynamic key. Each and every time the user gives his input it should generate a new key based on some cryptographic techniques and that will be used for future processing of the user identity. Hence we can ensure that there is high level of security measure is implemented and this will be provided by our proposed algorithm. This dynamic key will vary from user to user and they will be only known by the server.

	0	1	2	3	4	5	6	7	8	9
SERVER KEY:	6	2	8	1	0	4	3	9	5	7

Fig.No.4.Dynamic server key

ENCRYPTED ATM NUMBER:

We know that encryption technique is the most prominent method for any type of data hiding. Here the encryption is done along with water marking techniques where the newly generated ATM key will be watermarked in the fingerprint pattern that was generated at the initial stage. We can able to provide a double –shielded security for the ATM transactions.

WATERMARKED FINGERPRINT:

After the processing of all preliminary stages that we discussed, the final prospect is nothing but the watermarking of newly generated key from our proposed algorithm will be embedded into the fingerprint pattern. And that will be passed to the databases that are maintained by the server. Only this value is used for end transaction of the user.]

PROPOSED ALGORITHM:

Encryption(Input:user_pin[8],server_pat[16], random_key[8], Output: finger_array[16])

1. (i,j,k)← (0,0,0),finger_array[]←-1
// input key and modified input keys 2.
loop from i←0 to length(user_pin) // i
refers the user pin
3. loop from j←0 to length(server_pat)
// j refers the pattern that is generated by the
server
4. check user_pin[i]==j
// compare user pin with pattern at server
5. finger_array[i]←server_pat[j]
// store the values of server pattern in the
finger array
6. break loop
7.loop from i←8 to
length(finger_array) 8.
finger_array[i]←random_key[k]
// generate some random values
for the remaining fields
9. increment k.

Decryption(Input:finger_array[16],server_pat[
16] Output: user_pin[8])

1. (i,j)← (0,0)
2. loop from i←0 to
length(user_pin) 3.check if
finger_array[i]== -1
// check for blank
spaces 4.break
loop
5. else
6. loop from j←0 to length(finger_array)//
Retrieve pin number from watermarked
fingerprints
7.check if finger_array[i]== server_pat[j]
// verify the retrieved value with the
actual pin number.
8.user_pin[i] ←j

4. EXPERIMENTAL RESULTS:

The proposed approach has been applied to more than two hundred users pin numbers and the results are analyzed. Table No.1 shows some of the sample users pin numbers and their corresponding key that are uniquely generated by the server. In the existing system, the false match ratio is 0.13%.Table No.2 represents the improved accuracy of our proposed system.

Table No.1

PIN NUMBER	SERVER GENERATED
1456	1052364987
2548	8569231470
5689	8759326410
7536	8246759103
1035	0562387941

Table No.2

RATIO	PERCENTAGE
FALSE MATCH RATIO	0.01%
FALSE REJECTION RATIO	9.61%

5. CONCLUSION

In this method we have combined encryption and watermarking techniques to protect the identity of the user. Such a technique can help protect ATM users by taking their ATM Pin and their fingerprints as inputs. Watermarking their pin number after encryption in their corresponding fingerprint quadrant images helps in creating a new virtual identity for the user.

REFERENCES

[1] Khalil Zebbiche, LahouariGhouti, FouadKhelifi and Ahmed BouridaneProtecting Fingerprint Data using Watermarking "Protecting Fingerprint Data using Watermarking" First NASA/ESA Conference on Adaptive Hardware and Systems (AHS'06),IEEE computer society,2006, pp 451-456.

[2] AfzelNoore, Richa Singh, MayankVatsa, and Max M. Houck "Enhancing Security of Fingerprints throughContextual Biometric Watermarking**"**Elsevier Science 3 August 2006.

[3] BilgeGunsela, UmutUludag, A. Murat Tekalp "Robust watermarking of fingerprint images" Pattern Recognition vol.35, 2002,Elsevier, pp. 2739-2747

[4] Farid Ahmed & Ira S. Moskowitz,"Composite Signature Based Watermarking for Fingerprint Authentication" ACM Multimedia and Security Workshop, NY, NY August 1-2, 2005.

[5] Amr T. Abdel-Hamid ,SofiEneTahar, "A Survey on IP Watermarking Techniques"Springer Science, 9, pp.211–227, 2004.