Journal of Theoretical and Applied Information Technology
31st January 2014. Vol. 59 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

EFFICIENT TECHNIQUE TOWARDS THE AVOIDANCE OF REPLAY ATTACK USING LOW DISTORTION TRANSFORMS

[1]M.MANJU, [2]Dr.V.KAVITHA

[1]Assistant Professor, Department of CSE, Jayamatha Engineering College, Aralvaimozhi, India.

[2]Associate Professor, Department of CSE, University College of Engineering, Nagercoil,India.

E-mail: [1]mmanju_gem@yahoo.co.in ,[2]kavinayav@gmail.com

ABSTRACT

The huge number of fingerprints collected by the Federal Bureau of Investigation (FBI) has created an enormous problem in storage and transmission. Increase of online communication and transactions, has led to the requirement of security and privacy measures to be inbuilt in fingerprint recognition system. There are several solutions already in use to protect confidential information and to authenticate people electronically. When biometrics is used, it often deals with a discussion concerning privacy and integrity. This paper proposes a new methodology for effectively avoiding the replay attack during transmission of minutiae data. The minutiae information is split in to two parts and the first part is encrypted using pseudo-random permutation and then the remaining part of the minutiae information is embedded into the resultant permuted sequence using a low distortion based digital watermarking transform technique. To prove the integrity of the transmitted data, the receiver performs the same operation as that of the sender and compares the obtained data with the received data. Thus this algorithm gives solution to the replay attack which is found most common in all ATM based applications.

Keywords: *– Pseudo-Random Permutation, Digital Watermarking, Image Encryption, Low Distortion Transform.*

1.INTRODUCTION

Federal Bureau of Investigation (FBI) consists of a large volume of fingerprints containing more than 200 million cards, growing at a rate of 30,000- 50,000 new cards per day. These cards generally require greater storage space, and also their retrieval and transmission requires longer time. .In this new era of science and technology the main focus is given on providing solutions to the various attacks that are possible on data transmission. Security is considered to be the most critical factor in many applications. The main issues of such security based systems are integrity, privacy, authenticity and non-repudiation and these four issues are to be carefully addressed. In such applications only authorized users should have the access right for the related data. In centralized applications, the above said access control is handled by either a traditional user-id/password, or other more sophisticated access control mechanisms such as one-time password generators or smart tokens. For geographically distributed systems, the task of securing applications and data becomes extremely complex. In the modern society, to provide authentication, a positive determination or verification of personal identification is needed. There are a number of methods available for verifying the identity in an automated system.

Replay attack is a form of threat to integrity and it is defined as a type of active network attack in which a valid data transmission is maliciously repeated or delayed. This attack is carried out either at the source or by a third party who intercepts the data and retransmits it at some time later, which produces unauthorized effect. There are various countermeasure actions that can be taken to overcome from this type of attack. The first way to avoid replay attack is by using session tokens, which are selected randomly by a pseudo-random generator. The next way is the usage of one-time passwords, which are used to authenticate individual transactions and are commonly adopted in personal online banking systems. Nonce's along with a MAC code is also a way of avoiding replay attack. Time-stamping

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

is another way of preventing replay attack, where synchronization is achieved through a secure protocol. A typical method of resisting replay attacks consists of introducing time/session in the encrypted form which authenticates the source/destination of the encrypted transmission.

The paper is organized as follows: In Section 2 a brief literature survey on security of fingerprint data during transmission is discussed. Section 3 describes the proposed method for the avoidance of replay attack using low distortion transform based digital watermarking method. Section 4 analyses the performance analysis of the proposed methodology and finally in Section 5 the conclusion is discussed.

2. PREVIOUS WORKS

For eliminating replay attack, that is where a previously intercepted biometric is replayed, Ratha et al [1] proposed a challenge/response based system. A pseudo-random challenge is presented to the sensor by a secure transaction server. The sensor acquires the current biometric signal and computes the response for that challenge. Then, the acquired signal and the response computed are compared against the received signal in the transaction server for consistency. Soutar [2] projected a hill climbing attack for a simple image recognition system which is based on filter based correlation. Synthetic templates are gradually subjected as input to a biometric authentication system. Soutar also showed that the system could be compromised till the point of incorrect positive identification. J.Tian [3] introduced a difference expansion based reversible watermarking technique which creates space by expanding a difference. The data and the secondary information are further added to the expanded difference and get embedded in to the image. In this method the differences between adjacent pixels are doubled to generate a new Least Significant Plane (LSB) plane for accommodating additional data. A.M.Alattar al et al [4], L.Komsstra et.al [5] and D.Colluc et al [6] calculated the expanded difference by taking the difference between the adjacent pixels. D.M.Thodi et al [7] and V.Sachnev[8] presented a method in which the differences between the predicted pixels are taken in to account. C.C.Lee et al [9] developed a method for watermarking by considering the pixels of a block and the mean value of the block. To minimize the difference value the watermarking techniques are built on high performance predictors. M.Weinberger et al [10] hosted the JPEG-LS predictor which aims in reducing the difference value. Xinpeng Zhang [11] suggests a novel reversible data hiding scheme for encrypted data in which the data of the original cover is entirely encrypted and the additional message is embedded by modifying a part of the encrypted data

3. LOW DISTORTION TRANSFORM BASED DIGITAL WATERMARKING

In the proposed scheme, the parameters x, y and θ of fingerprint minutiae is first subjected to a pseudo-random permutation to produce the permuted sequence. Then the permuted sequence which contains the three parameters is used as carrier data for further watermarking. A low distortion transform based watermarking method is used to embed the parameters type, time and a RAND number generated by the server for every transaction. This embedded data along with the user information (Credit card number and pin number) and ATM center information are applied as input to MD5 to produce a 128 bit hash code. This hash code is concatenated with the encrypted version of embedded data and sent for transmission. In the receiving side, the ATM server on receiving the concatenated data, performs decryption process and then extracts type, time and RAND from the embedded data. After this recovery, the server performs validity check by using the time and RAND. If the comparison is not success, then the transaction is rejected by the server. Else it performs inverse permutation to generate the parameters x, y and θ. Then the four parameters x, y, θ and type are compared with the already stored fingerprint parameters as illustrated in Figure 1. If authenticated, the parameters are then subjected to permutation and embedding process which is as same as that of the sending side. The embedded data along with the user information (Credit card number and pin number) and ATM center information are applied as input to MD5 to produce a 128 bit hash code. This hash code is compared with the received hash code for proving integrity.

3.1 Sender Side Process-Atm Center

Journal of Theoretical and Applied Information Technology
31st January 2014. Vol. 59 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3.1.1 Permutation

The captured minutiae information consists of the co-ordinates (x, y), the angle (θ) and the type (bifurcation/termination). For encryption purpose, the parameters x, y and θ in digital form are imperiled to pseudo-random permutation to produce the permuted pixel sequence, which is considered as the encrypted data. A number of permutation based methods can be used here. In this encryption procedure, only the pixel positions are permuted and the pixel values are not masked.

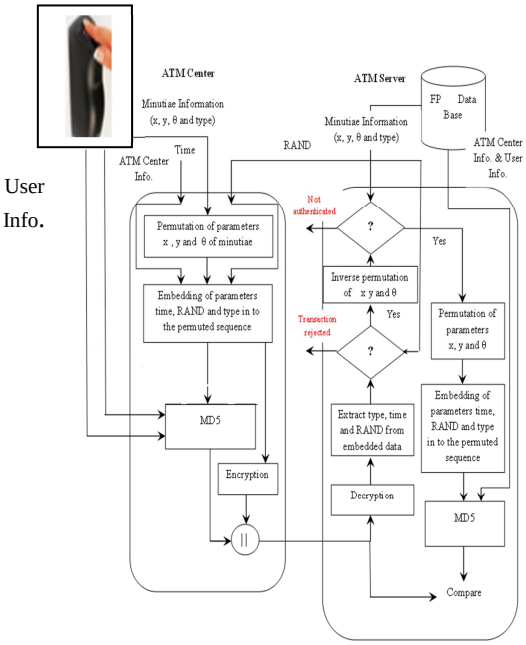

Figure 1: Architecture for Fingerprint Integrity

3.1.2 Embedding

The permuted sequence is first divided into two halves namely L part and H part. Instead of sending H part directly with the L part, the residual value is calculated and added with it. For doing so, first estimate/predict the H part from the L part using any nearest neighbor method to produce H_{est}. Then the residual is calculated as residual = H - H_{est}. Append the residual with the L part for further embedding. Embed type, time and RAND into the above sequence using Low distortion transform algorithm. Thus the space needed to store the three parameters is reduced through which compression is achieved. Since the algorithm produces low distortion during watermarking the receiver can reconstruct the original data without any loss of information.

3.1.3 Hashing

The parameters that are used for hashing are: embedded data, user information consisting of the 16 bit credit card number plus 4 bit pin number and ATM center information consisting of the location code for that center from GPS. Hashing algorithm like MD5 and SHA1 are used to produce the message digest or hash code whose size is 128 and 160 bits respectively. This hash code along with the encrypted form of the embedded data is now transmitted through the transmission line.

3.2 Receiving Side Process – Atm Server

3.2.1 Authentication Verification

3.2.1.1 Decryption and data recovery

The received data consists of the 128 bit hash code and the encrypted form of embedded data. First the ATM server performs decryption to obtain the embedded data. To recover the parameters type, time and RAND, reverse watermarking is performed.

3.2.1.2 Validation check

After extracting these parameters, the parameters time and RAND number are subjected to validation check. The validation check is carried out to check for replay by comparing the received time and RAND with that of the server. If validated, then the transaction is allowed else it is rejected.

3.2.1.3 Check for authentication

After validation check, inverse permutation is applied to get the original parameters x, y, and θ. From the server database, the parameters x, y and θ are mined out for the corresponding fingerprint and compared with the extracted parameters. If both get matched then the fingerprint is authenticated and allowed for further processing, else transaction gets terminated.

3.2.1.4 Check for replay attack and integrity

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The parameters x, y and θ are exposed to the permutation process and then embed type, time and RAND into the above permuted sequence using Low distortion transform algorithm. Then, hashing is performed for the same above said parameters to produce a 128 bit hash code. This hash code is compared with the received hash code and when a match is found, the data transmitted proves for a non-replay attack and also not modified.

3.3 Low Distortion Transform Algorithm (Data Hiding Algorithm)

The basic principle of this algorithm is to reduce the distortion introduced by the watermarking by embedding not only into the current pixel but also into its prediction context. For performing the algorithm, consider the linear predictor called the fourth predictor of JPEG. The proposed embedding scheme covers a 2 x 2 block. Let n, w and nw be the north, west and north-west neighbors of pixel x respectively as shown in Table 1.

Table 1 Pixel and their neighbors

NW	N
W	X

Algorithm 1 (Low Distortion Transform – Sender)

Input : Minutiae Information –x, y, θ, type, time, RAND

Step 1 : Pixel x is estimated as:

$\hat{x}$ = n + w – nw.

Step2 : The difference is calculated as :

p = x - $\hat{x}$

Step 3 : The prediction error $P_b = p + b$ where 'b' is the bit to be embedded.

Step 4 : Split P_b as evenly as possible in to four parts as d_x, d_n, $d_w$and d_{nw}. These values are calculated as follows:

$$d_x = \left\lfloor \frac{P_b}{4} \right\rfloor \quad d_w = \left\lfloor \frac{Pb+1}{4} \right\rfloor$$

$$d_{nw} = \left\lfloor \frac{Pb+2}{4} \right\rfloor \quad d_n = \left\lfloor \frac{Pb+3}{4} \right\rfloor$$

Here $\lfloor a \rfloor$ rounds 'a' towards minus infinity.

Step 5 :With this distributions, the new set of pixels become X, N,W and NW and are calculated as follows:

$$X = x + d_x$$
$$W = w + d_w$$

$$NW = nw + d_{nw}$$
$$N = n + d_n$$

Output: Embedded Data

Algorithm 2 (Low Distortion Transform – Receiver)

Input : Embedded Data

Step 1 : Pixel X is estimated as:

$\hat{X}$ = N +W – NW.

Step2 :The difference is calculated as:

P =X – $\hat{X}$ = 2p + b

Step 3 : Embedded data bit 'b' forms the LSB of X - $\hat{X}$

Step 4 : Recover p as p = $\frac{X - \hat{X} - b}{2}$

Step 5 :Compute d_x, d_n, $d_w$and d_{nw}as follows:

$$d_x = \left\lfloor \frac{P_b}{4} \right\rfloor \quad d_w = \left\lfloor \frac{Pb+1}{4} \right\rfloor$$

$$d_{nw} = \left\lfloor \frac{Pb+2}{4} \right\rfloor \quad d_n = \left\lfloor \frac{Pb+3}{4} \right\rfloor$$

Here $\lfloor a \rfloor$ rounds 'a' towards minus infinity.

Step 5 : Finally the original pixels are recovered as follows:

$$x = X - d_x$$
$$w = W + d_w$$

$$nw = NW - d_{nw}$$
$$n = N + d_n$$

Output: Reconstructed lossless minutiae information – x, y, θ, type, time, RAND

Journal of Theoretical and Applied Information Technology
31st January 2014. Vol. 59 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

4. RESULTS AND DISCUSSION

A fingerprint minutiae is represented with four parameters namely (x, y), which are the x and y co-ordinates of ridge ending or bifurcation and are represented by two bytes each. The other two parameters are θ, the angle and the type (0 for bifurcation and 1 for ridge ending). Four bytes for x co-ordinate, four bytes for y co-ordinate, one byte for angle and one bit for type are needed for processing. Sixteen minutiae points around the core point are chosen randomly for processing. Thus 144 bytes (16 x 9) is needed to represent the carrier data for embedding, which is then permuted. The parameters type (1 bit for each minutiae, so 16 bits), time (24 bits for time and 24 bits for date) and RAND number (16 bits) are used for embedding. Thus 80 bits of data gets embedded in 144 bytes of carrier date, thus reducing the storage space. About 25% of reduction is achieved with this watermarking scheme.MD5 hash algorithm is used for hashing. The message digest produced by MD5 algorithm is 128 bits. The inputs for hashing are: 144 bytes of embedded data, 32 bits of user information and 32 bits of center information. So a total of 156 bytes is applied as input to produce 128 bits hash code. This 128 bit hash code and the 144 byte encrypted embedded data are sent during transmission. Table 2 and Graph 1 analyses the time needed for recognizing the fingerprint from the database and the time needed to provide authentication for six different categories of fingerprint images from FVC 2002 database.

Table 2 Time Analysis For Each Category Of FVC 2002

Category	Query Name	Time for validation check (seconds)	Time for integrity check (seconds)
DB1-B	101-2.tif	5.398	5.421
	102-3.tif	5.895	5.9
	107-8.tif	5.865	5.985
DB1-B-3	101-3.tif	3.765	3.77
	104-2.tif	4.033	4.041
	106-7.tif	4.058	4.162
DB2-B	102-6.tif	3.771	3.776
	105-4.tif	4.012	4.018
	108-1.tif	4.202	4.213
DB3-B	102-5.tif	4.381	4.389
	105-4.tif	4.215	4.22
	108-1.tif	4.386	4.392
DB3-B1	101-2.tif	3.304	3.328
	104-2.tif	3.563	3.569
	106-6.tif	3.574	3.577
DB4-B	102-4.tif	3.842	3.849
	104-2.tif	3.31	3.316
	107-2.tif	3.372	3.883

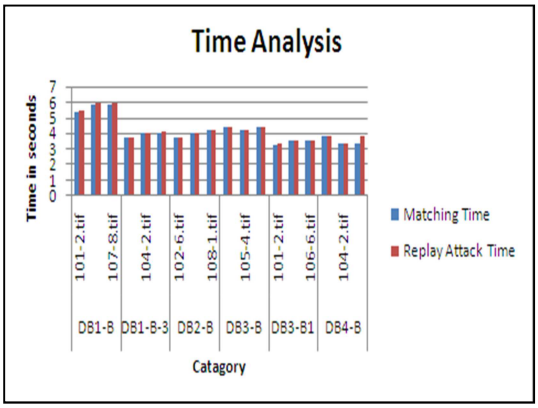

Figure 2: Time Analysis For Different Categories In FVC 2002 Database

Figure 3 depicts the False Accept Rate (FAR) and the False Reject Rate (FRR) of the different categories of fingerprint images from FVC 2002 database.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

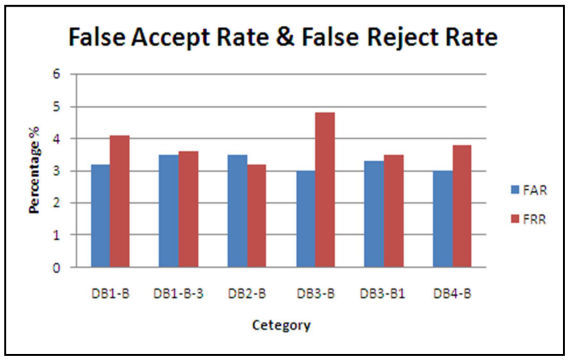

Figure 3: Analysis of FAR and FRR

5. CONCLUSION

In this paper, a low distortion transform for prediction error expansion reversible watermarking has been incorporated for hiding the minutiae parameters type, time and RAND in to the permuted sequence of the parameters x, y and θ . This embedded data along with the user information and center information are hashed using MD5 to yield the hash code at the sending side and it is transmitted along with the encrypted form of the embedded parameters. At the receiving side, the server accomplishes validation check and authentication check and if it is validated and authenticated, then it performs the same operation as that of the client and produces the message digest, which is compared with the received code for similarity, which proves for integrity of data and also it proves to be a way of resisting the replay attacks which are common in all banking applications.

REFERENCES:

[1]. N.K.Ratha, J.H.Connell and R.M.Bolle, "Enhancing security and privacy in biometrics-based authentication systems", IBM Systems Journal, vol.40, no.3, pp.614-634, 2001.

[2]. C.Soutar, "Biometric system security", http://www.bioscrypt.com.assets/security_soutar.

[3]. J.Tian," Reversible data embedding using a difference expansion", IEEE Trans. Circuits Syst. Video Technol., vol.13,no.8, pp.890-896, August 2003.

[4]. A.M.Alattar," Reversible watermark using the difference expansion of a generalized integer transform", IEEE Trans. Image Process, vol.13, no.8, 1147-1156, August 2004.

[5]. L.Kamstra and H.J.A.M.Heijmans, "Reversible data embedding in to images using wavelet techniques and sorting", IEEE Trans. Image Process, vol.14, n0.12, pp.2082-2090, December 2005.

[6]. D.Coltuc and J.M.Chassery," Very fast watermarking by reversible contrast mapping", IEEE Signal Processing Lett., vol.14, no.4, pp.255-258, April 2007.

[7]. D.M.Thodi and J.J.Rodriguez," Expansion embedding techniques for reversible watermarking", IEEE Trans. Vol.14, no.3, pp.721-730, March 2007.

[8]. V.Sachnev, H.J.Kim, J.Nam, S.Suresh, Y.Q.Shi, "Reversible watermarking algorithm using sorting and prediction", IEEE Trans. Circuits Syst. Video Technology, vol. 19, no.7, pp.989-999, July 2009.

[9]. C.C.Lee, H.C. Wu, C.S.Tsai and Y.P.Chu, "Adaptive lossless steganographic scheme with centralized difference expansion", Pattern Recognition, vol.41, no.6, pp.2097-2106, June 2008.

[10]. M.Weinberger, G.Seroussi and G.Sapiro," The LOCO- I lossless image compression algorithm: Principles and standardization in to JPEG-LS", IEEE Trans. Image Process., vol.9, no.8, pp.1309-1324, August 2000.

[11]. Xinpeng Zhang," Reversible data hiding in Encrypted image", IEEE Signal Processing Letters, vol.18, No.4. April 2011.

[12]. DinuColtuc,"Low distortion transform for reversible watermarking", IEEE Transactions on Image Processing, vol.21, no.1, pp.412-417, January 2012.

[13]. Xinpeng Zhang," Lossy compression and Iterative reconstruction for encrypted image", IEEE transactions on Information Forensics and Security, Vol.6, No.1,pp.53-58, March 2011.