APPLYING CRYPTOGRAPHY TO CANCELLABLE SIGNATURES

Shiwani Gupta
TCET

Abstract- **Biometric characteristics are largely immutable, i.e. unprotected storage of biometric data provokes serious privacy threats, e.g. identity theft, limited re-newability, or cross-matching. Once compromised, biometric traits cannot be canceled or reissued. To handle above issues in case of behavioral biometric-signatures, I propose to generate a non-invertible cryptographic key from cancelable online signature templates. Initially, a noninvertible transformation is applied on the grid and texture features extracted from online signatures. Subsequently, the transformed points form cancelable templates which are then utilized to generate a unique non-invertible key. As the cryptographic key generated is non-invertible, it is highly infeasible to acquire the cancelable signature templates or the original signature from the generated key.**

***Index Terms*— online signature; cancellable biometrics; non invertible transform; cryptography; pattern recognition**

I. INTRODUCTION

With the widespread diffusion of biometrics-based recognition systems, there is an increasing awareness of the risks associated with the use of biometric data. Significant efforts are therefore being dedicated to the design of algorithms and architectures able to secure the biometric characteristics, and to guarantee the necessary privacy to their owners.

Unlike password or tokens, if a biometric is compromised, it cannot be revoked or reissued. Hence non invertible transformations are applied to the acquired biometrics, making impossible to derive the original biometrics from the stored templates, while maintaining the same recognition performances of an unprotected system.

Secondly, a biometric matcher has to consider the variability of biometric data, as two acquisitions of an identical biometric trait are rarely identical due to differences in alignment, missing/spurious features and differences in values of features that are present in both acquisitions. Further large interclass similarity complicates the feature extraction and matching problem. There is a tradeoff b/w FMR (False Match Rate) and FNMR (false Nonmatch Rate). If threshold is decreased to make the system more tolerant to biometric intraclass variability, FMR increases; whereas if threshold is increased to make the system more secure, FNMR increases.

II. ONLINE SIGNATURE

Human Signature is proven to be the most natural, widely accepted[1,2] biometric attribute of a human being which can be used to authenticate human identity and is even less intrusive and has no negative or undesirable health connotations[3]. But great variability can be observed in signatures according to country, age, time, habits, psychological or mental state, physical and practical conditions[4]. Intrapersonal variations and Interpersonal differences make it necessary to analyze them as complete images and not as letters and words put together[1].

Offline systems are more applicable and easy to use in comparison with on-line systems which are more unique and difficult to forge[5], however it is considered more difficult to design offline than on-line due to the lack of dynamic information such as no. of strokes, velocity etc. Although a great amount of work has been done on random and simple forgery detection, more hard work is still needed to tackle the problem of skilled forgery detection.

The choice of a powerful set of features is crucial in signature verification systems. The features that are extracted are used to create a feature vector which is then used to uniquely characterize a candidate signature. In [6] texture features in signature template give information about occurrence of specific pen tip pressure pattern while signing and can be extracted by the algorithm in Figure1.

1. Scan the signature pressure template. Divide the template into five sub-template with pressure level range R1 = (0- 20), R2 = (21-40), R3 = (41-60), R4 = (61-80) and R5 = (81-100). Start with Template R1.
2. Define the displacement vector. d= (dx, dy).
3. Start scanning the signature sub-template segments 1 to segment 16.
4. Find the co-occurrence of pixel sets c00, c01, c10 & c11 for the displacement vector dx, dy for the segments defined in step 3. Where 0 indicates pressure level P1 and 1 indicates Pressure Level P2.
5. Repeat the procedure for all the 16 segments, and all pressure ranges. Store the values in specific memory structure.
6. When all the segments are scanned, select other displacement vector and repeat steps 3 to 5. This is repeated for all four displacement vectors (1,0),(1,1),(0,1),(-1,-1).
7. Select element c01 and c11 of the matrix for each displacement vector.
8. This procedure gives total 128 X 5 = 320 elements as follows (16 segments X 4 matrices X 2 elements per matrix X 5 Ranges). This forms the texture feature vector.

Figure 1. Extraction of texture features

Then grid features provide information about pixel density and are extracted from signature template using algorithm in Figure2.

The third feature is statistical feature derived from centre of mass of an image segment. The algorithm is shown in Figure 3. We split the template and find the geometric center of mass of each generated segment and again split the template at the center of mass. This process is repeated 15 times to generate 24 points and carried over in two modes - horizontal and vertical splitting. In one level we split the template 3 times and obtain 6 points and 4 segments, these 4 segments are split again and to generate total 6*4= 24 points. Hence the name successive geometric centers of depth 2. Total 24 vertical and 24 horizontal feature points are generated to compare two signatures.

1. Divide the skeletonized image into 10 X 10 pixel blocks.
2. For each block segment, calculate the area (sum of pressure pixels). This gives a grid feature matrix (gf) of size 25 X 25.
3. Find minimum and maximum (min, max) values for pixels block. Ignore blocks with no pixels.
4. Normalize the grid feature matrix by replacing each nonzero element. This gives matrix with all elements within the range of 0 and 1.
5. The resulting 625 elements of the matrix (gf) form the grid feature vector.

Figure 2. Extraction of grid features

```
1. Read the interval points (x1,y1) and (x2,y2)
if (x1 > x2) then exchange the points
Set the flag reverse = true
2. Calculate the difference
dx = x2 - x1        dy = y2 - y1
3. If |dx| > |dy|
then      m = dy / dx        y = y1
          Calculate the points between X1 & X2 by
          for (x = x1; x < x2; x++)
          Xi = Round(x)    Yi = Round(y)
          Store Xi,Yi to array Points[,]
          y = y + m
else      Go to Step 4
Go to Step 6
4. If |dx| < |dy|
then      m = dx / dy        x = x1
          if (y1 < y2)
          then      Calculate the points between Y1
                    & Y2 by
                    for (y = y1; y < y2; y++)
                    Xi = Round(x)    Yi = Round(y)
                    Store Xi,Yi to array Points[,]
                    x = x + m
           else     Go to Step 5
Go to Step 6.
5. If (y1 > y2)
then      Calculate the points between Y1 & Y2 by
          for (y = y1; y > y2; y--)
                    Xi = Round(x)    Yi = Round(y)
                    Store Xi,Yi to array Points[,]
                    x = x - m
6. If reverse flag is set then Rearrange the Points[,]
array in reverse order.
7. Insert the points (Xi,Yi) from Points[,] array into
the main signature features array between Pi &
Pi+1
```

errors due to sampling, quantization, speed of hardware, signing position etc. As the digitizer has finite rate of sampling and data transfer, it cannot capture all the points on a curve but captures finite points as per the sampling rate. Hence there is loss of continuity in the captured points. If the signing speed is high then the captured points are less. Hence interpolation is required via MDDA (Modified Digital Difference Analyzer) algorithm. DDA is mainly used in CG for line drawing on raster. We use this algorithm for finding missing points between the two interval points, these points are actually on a curve but as the distance between two points is very small (generally 0 to 4 pixels maximum), hence the points can be assumed on a line and DDA can be used for calculation of points which lie on a line between two given points (x1,y1) and (x2,y2).

The signature points have temporal locality means the consecutive points tend to have similar value as their neighbors. The maximum packet rate is 200 packets/seconds; it has been observed that the time difference between two sampled points varies from 5ms to 10ms. Hence we use this fact to interpolate the other parameters.

III. SECURING SIGNATURE

Signature Recognition can provide continued authentication without introducing extra work to a user and they are much more difficult to steal by an impostor but false rejection rate (FRR) can be very high if a user makes sudden behavior changes. Hence to tackle problems of noise and intra-class variations; biometric data needs to be protected with cryptography. Typically, there are two goals in securing biometric data. The first goal is to achieve the one-way transformation from raw image to template: it should be computationally difficult to regenerate a raw image from a template. The second goal is to generate multiple independent biometric templates from one image in order to reuse the biometric [7].

These goals are accomplished by cancellable biometrics which refers to the intentional and systematically repeatable distortion of biometric features in order to protect sensitive user-specific data. If a cancelable feature is compromised, the distortion characteristics are changed via auxiliary data and the same biometrics is mapped to a new template, which is used subsequently. Cancelable biometrics requires storage of the distorted version of the biometric template which provides high privacy level by allowing multiple templates to be associated with the same biometric data. A distinct advantage of cancelable biometric compare to other biometric template techniques such as biometric cryptosystem is that the transformed biometrics can remain in the same feature space of the original ones, so that the same matcher can be used for authentication.

In [8] authors propose a provably secure, registration-free construction of cancelable fingerprint templates based on localized, self-aligned texture features and then we demonstrate how to construct cancelable templates from them. In [9] authors have concluded that feature-level cancelable biometric construction is practicable in large biometric deployments. They empirically compare the performance of several algorithms such as Cartesian, polar, and surface folding transformations of the minutiae positions. It is also shown that the transforms are noninvertible by demonstrating that it is computationally hard to recover the original biometric identifier from a transformed version.

A person only has two irises - if his pattern is stolen he quickly runs out of alternatives. Thus methods that protect the true iris pattern need to be adopted in practical biometric applications. In particular, it is desirable to have a system that can generate a new unique pattern if the one being used is lost, or generate different unique patterns for different applications to prevent cross-matching. For backwards compatibility, these patterns should look like plausible irises so they can be handled with the same processing tools. However, they should also non-invertibly hide the true biometric so it is never exposed, or even stored. In [10] biometric methods are proposed either at the unwrapped image level or at the binary iris code level

In [11] alignment-free cancelable iris biometrics based on adaptive Bloom filters are proposed which enable an efficient alignment-invariant biometric comparison while a successive mapping of parts of a binary biometric template to a Bloom filter represents an irreversible transform.

In [12], an ICA coefficient vector is extracted from an input face image. Some components of this vector are replaced randomly from a Gaussian distribution which reflects the original mean and variance of the components. Then the vector with its components replaced, has its elements scrambled randomly. A new transformed face coefficient vector is generated by choosing the minimum or maximum component of multiple (two or more) differing cases of such transformed coefficient vectors.

Biometric data are intrinsically not identically reproducible (we measure a distance between samples) and nonuniformly distributed (e.g. only one nose, in the middle of the face). More realistic, biometric data being never identically reproducible, one could use a biometric capture as a source of randomness to generate keys in cryptography by hashing[13,14] the captured data for instance. Secondly, biometric data has to be saved in a centralized database or distributed on smart cards. Potential users of biometrics are unwilling to give out their biometric data because they are concerned how their biometric data will be used, for what purpose, and whether their biometric data will be protected sufficiently. Hence the biometric data needs to be protected with cryptography.

There are two variants: Biometrics based key release (The matching operates on traditional biometric templates, if they match, the cryptographic key is released from its secure location), Biometrics based key generation (Biometrics and cryptography are merged together at a deeper level. The matching extracts key from conglomerate data).

In [15] an algorithm is proposed for deriving the key from fingerprint for ECC (Elliptic Curve Cryptography) based applications. The proposed approach reduces the cost associated with lost keys, addresses non-repudiation issues and provides increased security of digital content.

In [16] authors have presented a secure way to integrate iris biometric with cryptography. Biometric key is generated from iris code. Proposed a feature level fusion network based on fuzzy vault[17] and fuzzy commitment scheme[18].

In [19] a biometric cryptosystem which uses online signatures, based on the fuzzy vault scheme of Jules et al. is proposed The fuzzy vault scheme releases a previously stored key when the biometric data presented for verification matches the previously stored template hidden in a vault. They extract minutiae points (trajectory crossings, endings and points of high curvature) from online signatures and use those during the locking & unlocking phases of the vault.

IV. APPLYING CRYPTOGRAPHY TO CANCELLABLE SIGNATURES

On one hand, a drawback of Cancellable Biometrics such as the ones used for fingerprints, tends to break the underlying structure, thus degrading the performance accuracy. On the other hand, cryptography reduces matching to error correction. Moreover, the security's advantages of both schemes adds up together [20].

The principal drawback of the existing cryptographic algorithms is the maintenance of their key's secrecy. Added with, human users have a difficult time remembering strong but lengthy cryptographic keys. As a result, utilizing individual's biometric features in the generation of strong and repeatable cryptographic keys has gained enormous popularity among researchers. The unpredictability of the user's biometric features, incorporated into the generated cryptographic key, makes the key unguessable to an attacker lacking noteworthy knowledge of the user's biometrics. Nevertheless, if a person's biometric is lost once, it will be compromised forever as it is inherently associated with the user. To overcome the above, cancelable biometrics has been proposed as an effective solution for canceling and re-issuing biometric templates.

In [21], authors have projected an approach to produce irrevocable cryptographic key from cancelable fingerprint templates. It is extremely unfeasible to obtain cancelable fingerprint templates and original fingerprints from the generated key since the cryptographic key produced is irrevocable.

The work done in area of cancellable biometrics, biocryptic systems and the combination involve fingerprint or iris or face. Researchers haven't shown much work in the area of securing signature biometric. Hence, I propose to generate a non-invertible cryptographic key from cancelable online signature templates. Initially, a one-way transformation as Hadamard or Baker or biohash would be applied on the texture, grid and statistical features extracted from online signatures via WACOM tablet. Subsequently, the transformed points are made use of to form cancelable templates. The cancelable templates are then utilized to generate a unique non-invertible key. As the cryptographic key generated is non-invertible, it would be highly infeasible to acquire the cancelable signature template or the original signature from the generated key.

ACKNOWLEDGMENT

I would like to pay my deep gratitude to my friend and HOD IT, TCET, Mumbai, who guided me whenever I got stuck somewhere.

REFERENCES

[1] M.S. Arya, V.S. Ianmdar, "A Preliminary Study on Various Off-line Hand Written Signature Verification Approaches" International Journal of Computer Applications (0975 – 8887) Volume 1 – No. 9 2010.

[2] Vu N., Blumenstein, M., Muthukkumarasamy V., Leedham G., "Off-line Signature Verification Using Enhanced Modified Direction Features in Conjunction with Neural Classifiers and Support Vector Machines", in Proc. 9th Int Conf on document analysis and recognition, vol 02, pp. 734-738, Sep 2007.

[3] MI C.F., "Signature verification revisited: promoting practical exploitation of biometric technology", Electronics & Communication Engineering Journal, December 1997.

[4] H. Anand, D.L. Dhombe, "Relative study of signature verification and recognition system", International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163 Volume 1 Issue 5 (June 2014).

[5] R. Abbas and V. Ciesielski, "A Prototype System for Off-line Signature Verification Using Multilayered Feed forward Neural Networks," February 1995.

[6] V.A.Bharadi, R.R. Sedamkar, P.S.Jangid, "Performance analysis of grid and texture based feature vector for dynamic signature recognition", IEEE, 2015, Pune.

[7] Q. Gao, "Biometric authentication to prevent e-cheating", Vol 9 No.2, IJITDL, Feb 2012.

[8] Chikkerur S., Ratha N.K., Connell J.H., Bolle R.M., "Generating Registration-free Cancelable Fingerprint Templates", 2nd IEEE International Conference Biometrics: Theory, Applications and Systems, 2008.

[9] Ratha N.K., Res. H., Chikkerur S., Connell J.H., Bolle R.M., "Generating cancellable fingerprint templates", IEEE Transactions on Pattern Analysis and Machine Intelligence, (Volume:29 , Issue: 4)

[10] J. Zuo, Ratha, N.K., Connell, J.H. "Cancellable iris biometric", IEEE International conference on Pattern Recognition, ICPR 2008, Tampa FL.

[11] Rathgeb C., Breitinger F., Busch C., "Alignment-free cancelable iris biometric templates based on adaptive bloom filters", IEEE International Conference on Biometrics Compendium, ICB 2013, IEEE, Madrid.

[12] M.Y. Jeong, A. B. J. Teoh "Cancellable Face Biometrics System by Combining Independent Component Analysis Coefficients", 4th International Workshop, IWCF 2010, Tokyo, Japan.

[13] A. Teoh, A. Goh, D. Ngo, "Random multispace quantization as an analytic mechanism for biohashing of biometric and random identity inputs," Pattern Analysis and Machine Intelligence, IEEE Transactions on, vol. 28, no. 12, pp. 1892 –1901, Dec. 2006.

[14] L. Nanni, A. Lumini, "Empirical tests on biohashing," Neurocomputing, vol. 69, no. 16-18, pp. 2390 – 2395, 2006.

[15] B. R. Rao, Dr. E.V.V.K. Rao, S.V.R. Rao, M.R.M. Rao, "Finger Print Parameter Based Cryptographic Key Generation", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 6, November- December 2012, pp.1598-1604.

[16] F. Hao, R. Anderson, J. Daugman. "Combining cryptography with biometrics effectively", IEEE transaction, volume 55, issue 9, pp 1081- 1088,2006 .

[17] M. AlTarawneh, W. Woo, S. Dlay, "Fuzzy vault crypto biometric key based on fingerprint vector features," 6th International Symposium on Communication Systems, Networks and Digital Signal Processing, 2008, pp. 452 –456.

[18] A. Juels, M. Wattenberg, "A fuzzy commitment scheme," in Proc. ACM Conf. on Computer and Communications Security, pp. 28–36, 1999.

[19] A. Kholmatov, B. Yanikoglu, "Biometric cryptosystem using online signatures". International Conference on Computer & Information Sciences, volume 4263 , pp 981-990,2006 .

[20] J. Bringer, H. Chabanne, B Kindarji, “The best of both worlds: Applying secure sketches to cancellable biometrics”, 2008, Science Direct.

[21] Lalithamani N., Soman S.T. “Towards generating irrevocable key for cryptography from cancelable fingerprints“, 2nd IEEE International Conference on Computer Science and Information Technology, 2009. ICCSIT.