Adapting Biometric Representations for Cryptosystems

Anil K. Jain

With

Abhishek Nagar & Karthik Nandakumar

Department of Computer Science and Engineering

Michigan State University

http://biometrics.cse.msu.edu

Outline

- Biometric systems
- Security of biometric systems
- Biometric cryptosystems
  - Fuzzy commitment & fuzzy vault
  - Alignment
  - Adapting representations
  - Hybrid cryptosystems
- Challenges

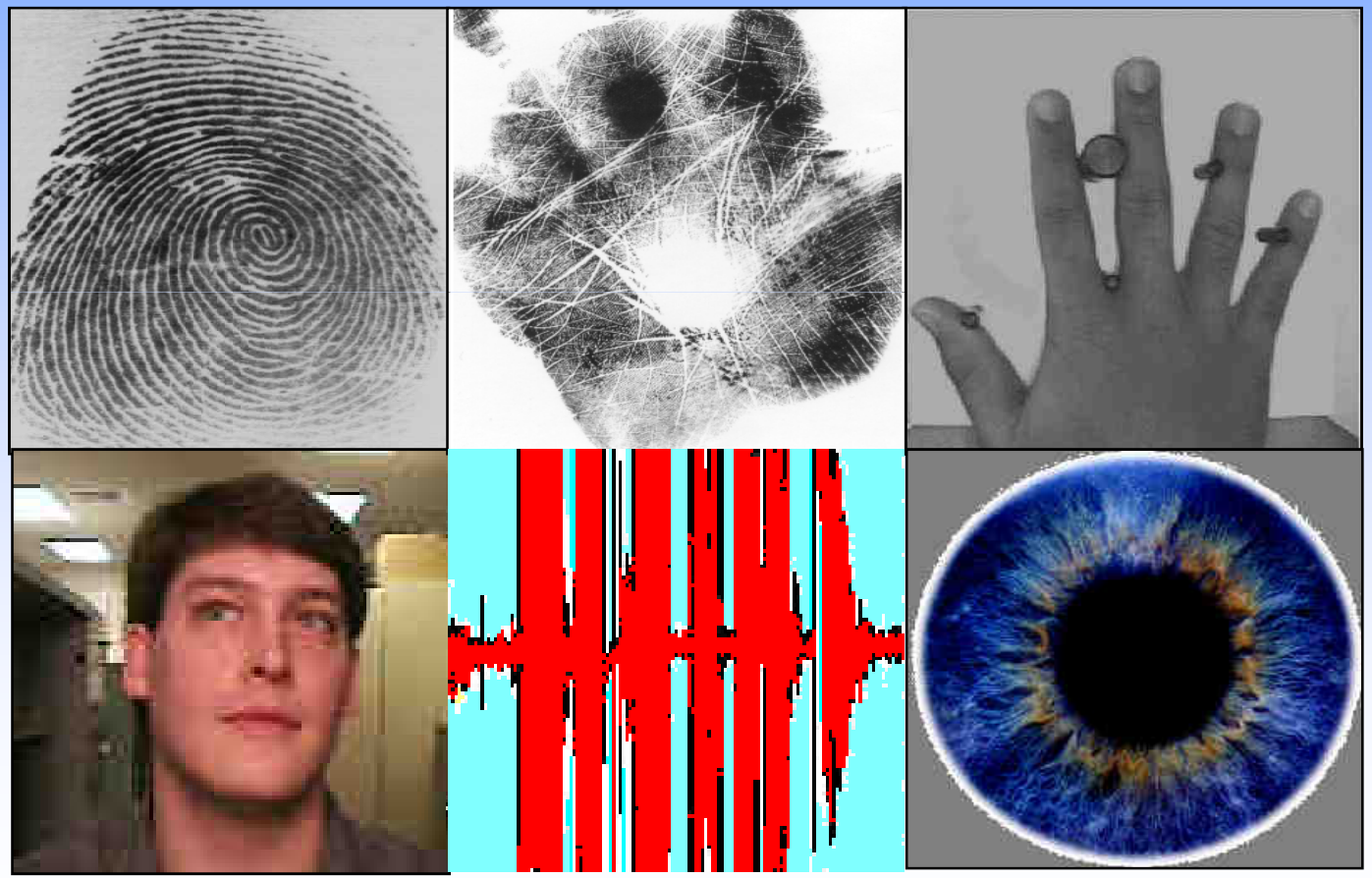
User Authentication

- Users can no longer be trusted based on credentials
  - Most popular password is "123456"
    - Skimming, phishing
  - "For terrorists, travel documents are as important as weapons"[1]
    - Spanish police arrested 7 men, connected to al-Qaeda, tasked with stealing 40 passports/month[2]
- But, credentials can be revoked and reissued

[1] http://www.9-11commission.gov/report/911Report.pdf (pg. 384, 2nd paragraph)
[2] http://homelandsecuritynewswire.com/spain-busts-terrorist-passport-stealing-ring

Biometric Recognition

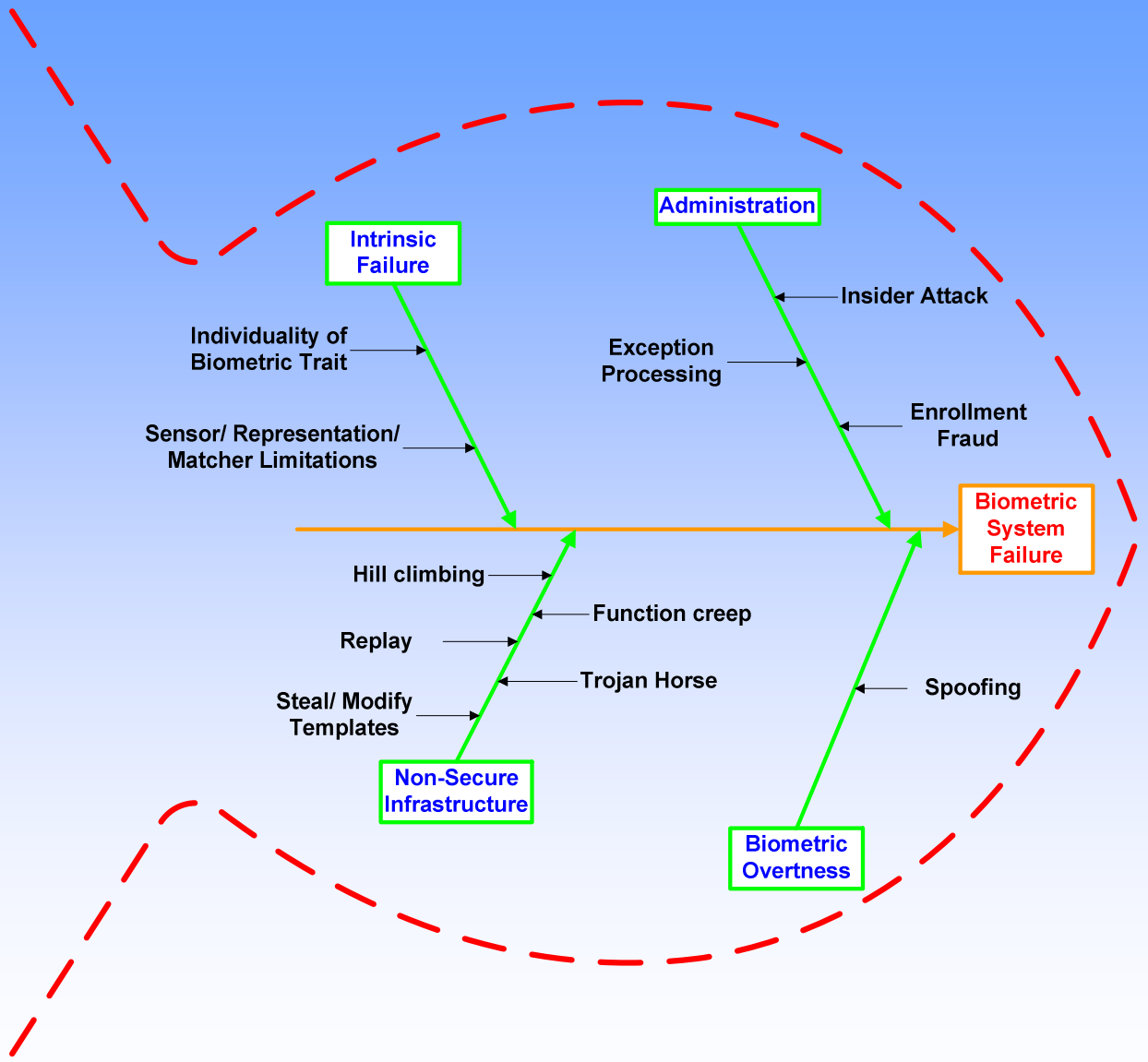
Automatic method for person recognition based on one or more intrinsic physical or behavioral traits



Fundamental Premise

- Biometric traits are unique & permanent!
  - Intra-class variability is extremely small
  - Inter-class variability is extremely large
- In practice, systems have non-zero FAR & FRR

System Vulnerabilities



Template security is one of the most critical issues

Template Security

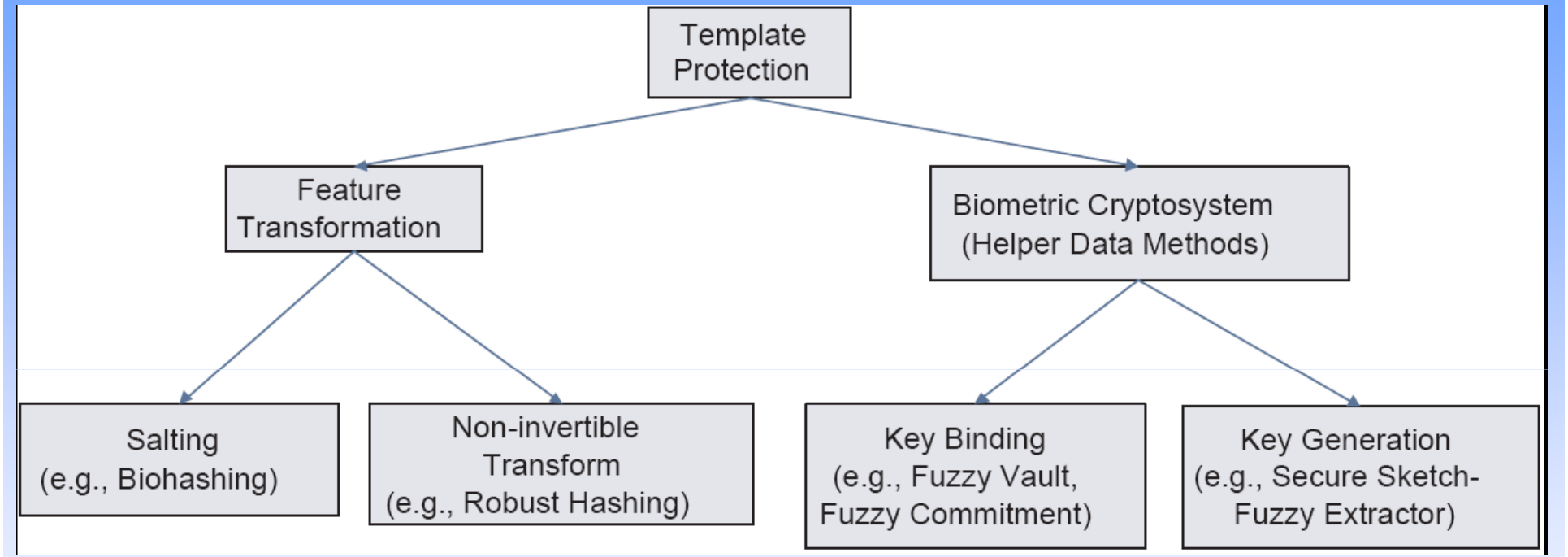
- Consequences of stolen templates
  - Intrusion: create physical spoof (security vulnerability)
  - Function creep: cross-matching (loss of privacy)

Secure Template: Requirements

- Diversity: Secure template must not allow cross-matching, ensuring user's privacy
- Revocability: Revoke a compromised template and reissue a new one using the same biometric
- Security: Difficult to obtain the original template from the secure template
- Performance: Secure template should not degrade the matching performance

Challenge: How to satisfy all these requirements at the same time in the presence of intra-user variations?

Secure Template: Approaches

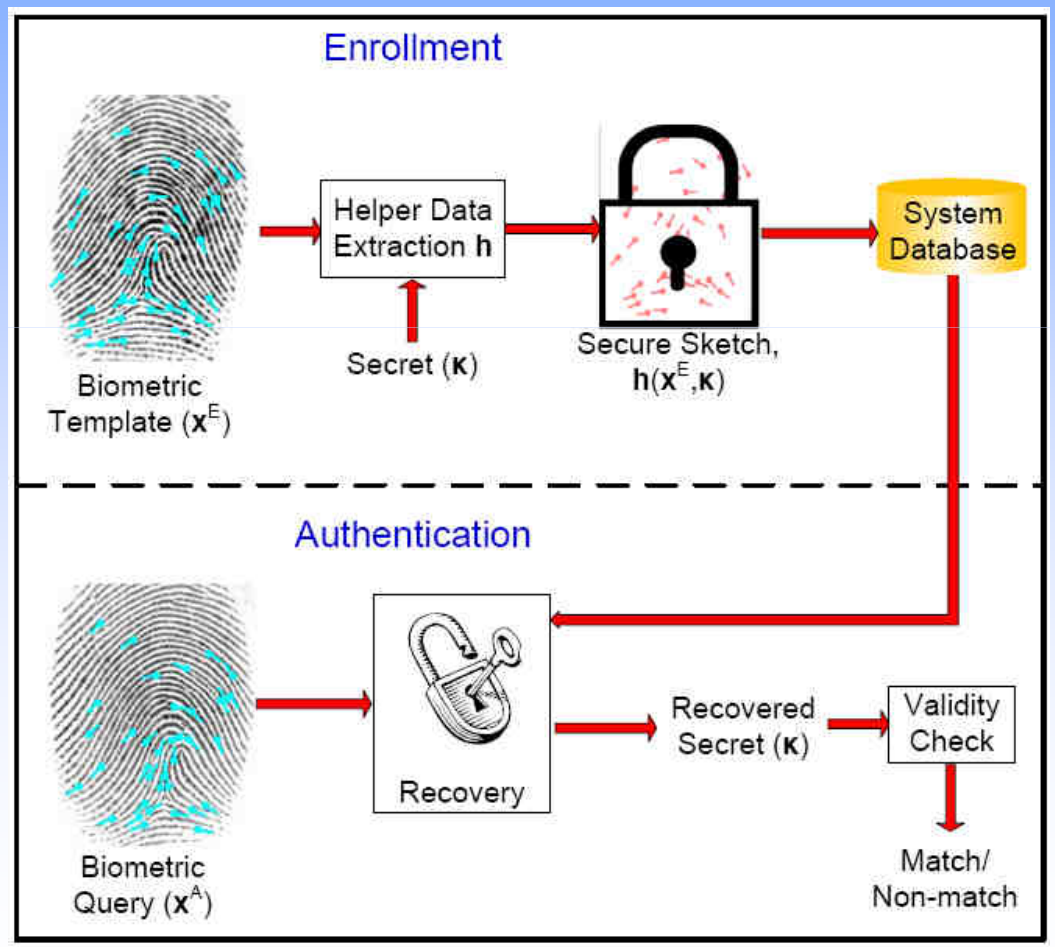


- Hybrid schemes: make use of more than one basic approach e.g., salting followed by key binding

Jain, Nandakumar and Nagar, "Biometric Template security", EURASIP J. on Advances in Signal Processing, 2008

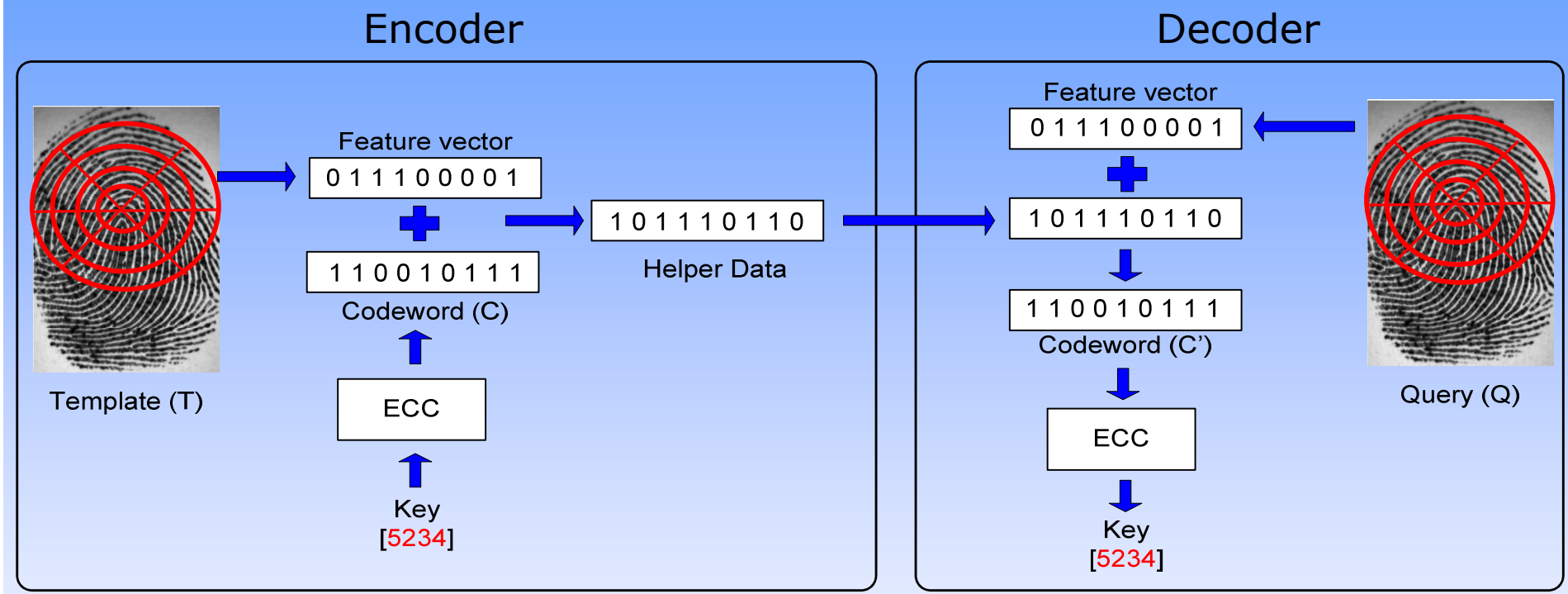
Key-binding Biometric Cryptosystem

- Store a secure sketch (helper data) by biding the template wit a cryptographic key



Fuzzy vault (point set features); fuzzy commitment (binary strings)

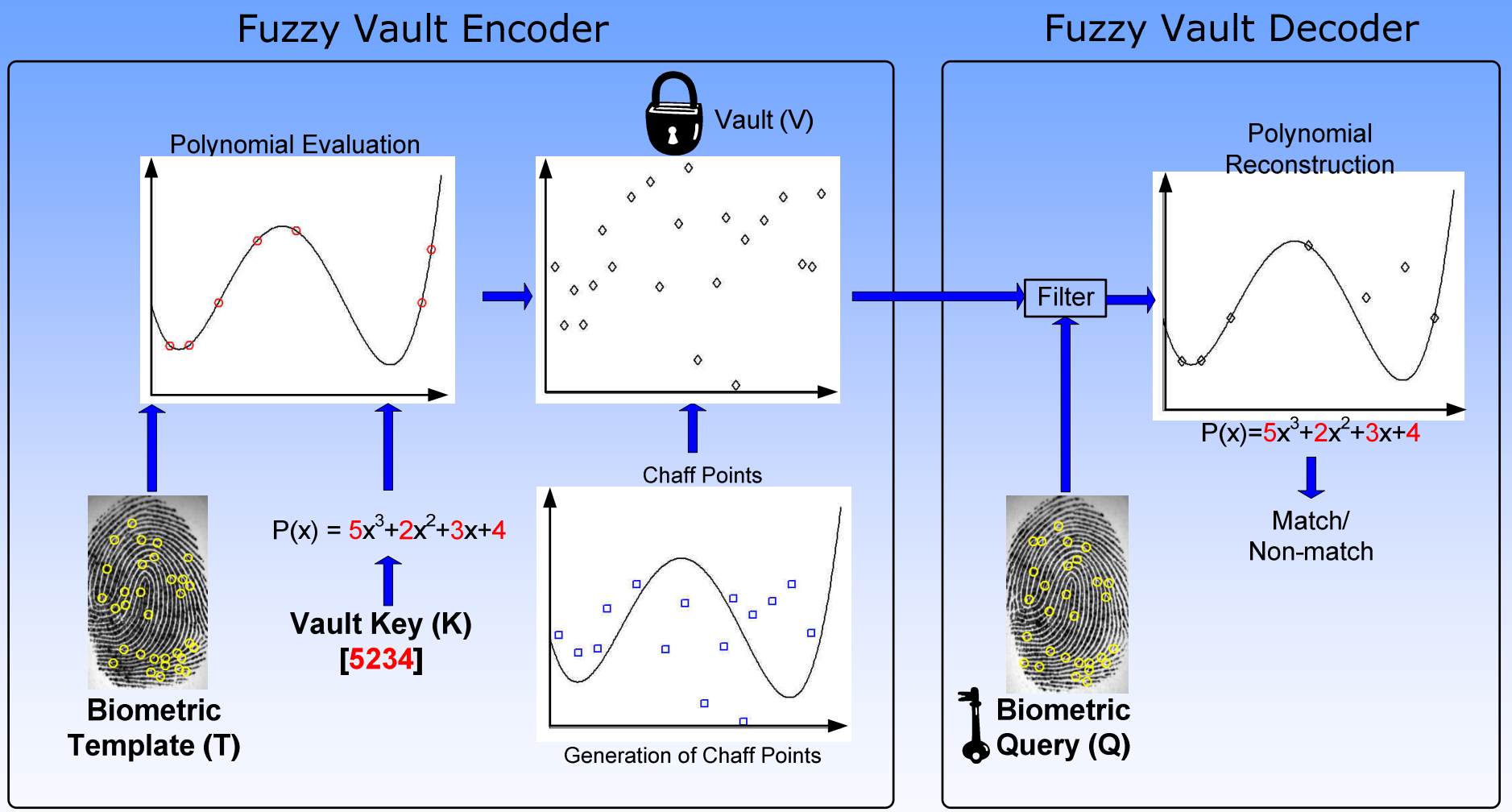
Fuzzy Commitment



- Variability in binary biometric features is translated to variability in codeword of an error correction scheme, which is indexed by a key
- Corrupted codeword can be corrected to recover the embedded key
- Lack of *perfect* code for desired code length

Juels and Wattenberg, "A fuzzy commitment scheme," in Proc. 6th ACM Conf. Computer and Communications Security, 1999

Fuzzy Vault



- Decoder identifies genuine points in mixture of genuine & chaff points
- How to generate chaff points that are indistinguishable from genuine points?

Nandakumar, Jain and Pankanti, "Fingerprint-based Fuzzy Vault: Implementation and Performance", *IEEE TIFS*, 2007

Fingerprint Vault

Fingerprint

Minutiae

Fuzzy vault

Fuzzy Schemes: Challenges

- How to align query with template without template leakage?
- How to construct vault/commitment for arbitrary biometric traits/representations?
- How to enable revocability?
- How to estimate security given that biometric features distributions are non-uniform?

Alignment

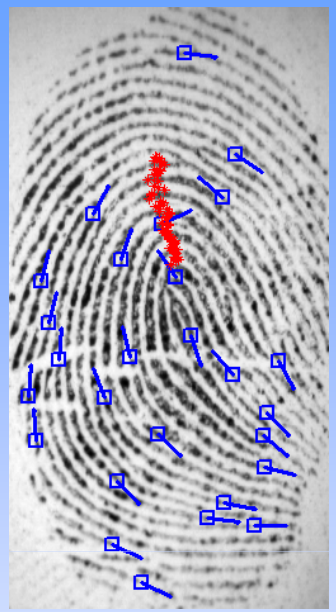
Three different impressions of the same finger

Template image or feature vector not available for alignment; additional data stored for alignment should

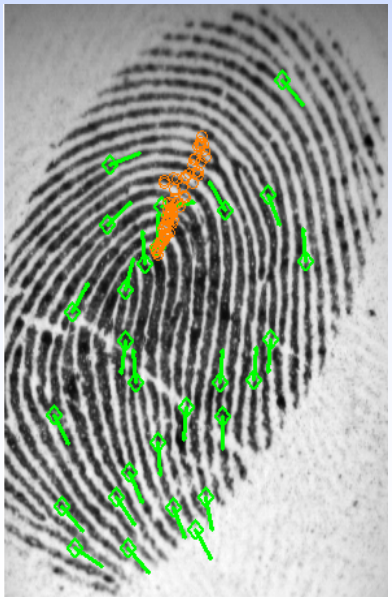
- not lead to template reconstruction
- carry sufficient information for alignment

Alignment based on High Curvature Points

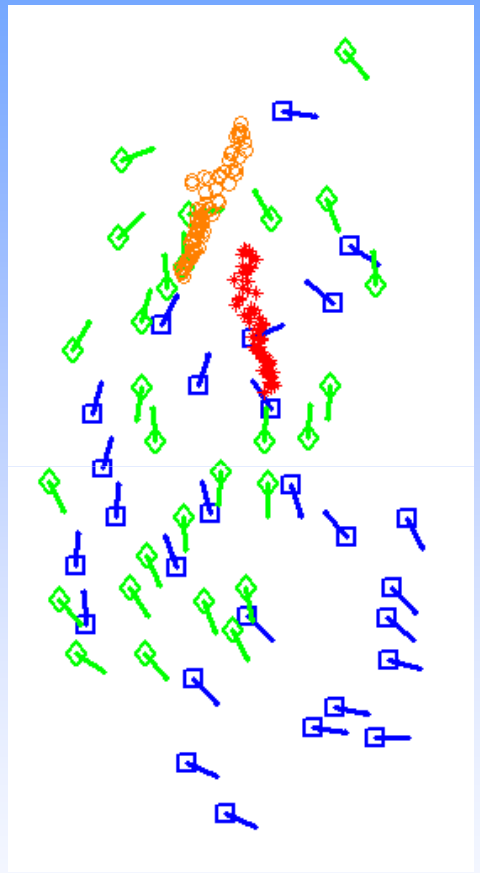
Template



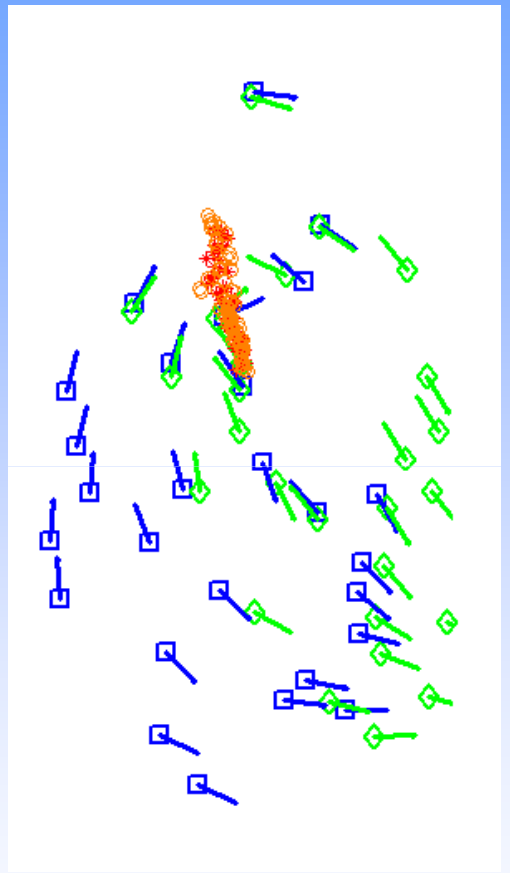
Query



Overlaid minutiae



Aligned minutiae



- High curvature points do not reveal the minutiae template
- Requires extra storage & computation

Nandakumar, Jain & Pankanti, TIFS, 2007

Focal-Point Based Alignment

- Focal point is the average centre of curvature of high curvature ridges; analogous to a core point
- Requires storage of a single (x,y,θ) point
- Can be extracted even for arch-type & partial prints

Nandakumar, "A fingerprint cryptosystem based on minutiae phase spectrum", WIFS, 2010

Other Secure Alignment Approaches

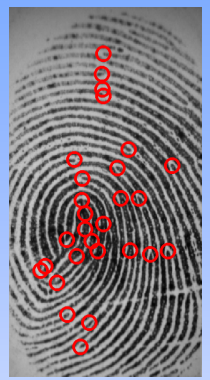
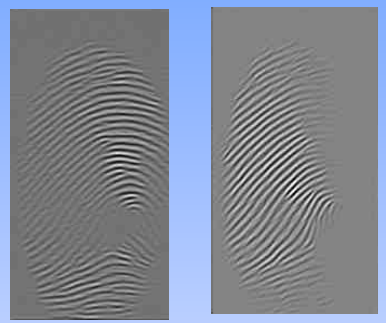
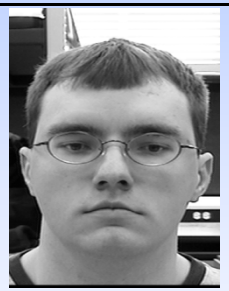
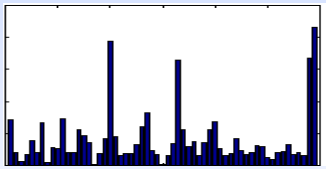
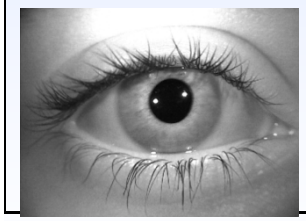
- Reliable minutiae neighborhood[1]
  - Requires training
- Singular points
  - Not always available
- Use of features relative to each minutiae[2]
  - Invariant to rotation and translation
  - Different matching approaches are needed
  - Difficult to analyze its security

[1] S. Yang and I. Verbauwhede, "Automatic Secure Fingerprint Verification System Based on Fuzzy Vault Scheme," ICASSP, March 2005
[2] T. E. Boult, W. J. Scheirer, and R. Woodworth, "Fingerprint Revocable Biotokens: Accuracy and Security Analysis," CVPR, June 2007

Adapting Biometric Representations

- Motivation
  - Obtain a representation in a form suitable for fuzzy commitment and fuzzy vault
  - Facilitate fusion of modalities
- Requirements
  - Maintain discriminability
  - Uniformly random features for security analysis

Biometric Representations

Trait	Features		Representation Type
	Minutiae 	Texture-based 	Minutiae: Unordered set of points, variable size, distribution is not uniform Texture-based (fingercode): Real-valued fixed-length vector, values are not i.i.d
	Subspace projections 	Local Texture (e.g., LBP) 	PCA/LDA/LBP Histogram: Real-valued fixed-length vector, values are not i.i.d
	Iriscode 		Fixed-length binary string; bits are not random and independent

Is it possible to have a common *efficient* representation?

Example of Adaptation

- Objective: Transform minutiae set into binary string

$$f(u,v)=\sum_{i=1}^{n}\delta(x-x_i,y-y_i)\exp(j\theta_i)$$

- Phase of Fourier spectrum is sampled on log-polar grid and quantized

$$\psi(F(u,v))=\arctan\frac{\sum_{i=1}^{n}\sin(2\pi(ux_i+vy_i)+\theta_i)}{\sum_{i=1}^{n}\cos(2\pi(ux_i+vy_i)+\theta_i)}$$

Fingerprint minutia set

Binarized Phase Spectrum (BiPS) representation adapted for fuzzy commitment

K. Nandakumar, "A Fingerprint Cryptosystem Based on Minutiae Phase Spectrum", IEEE WIFS, Dec 2010.

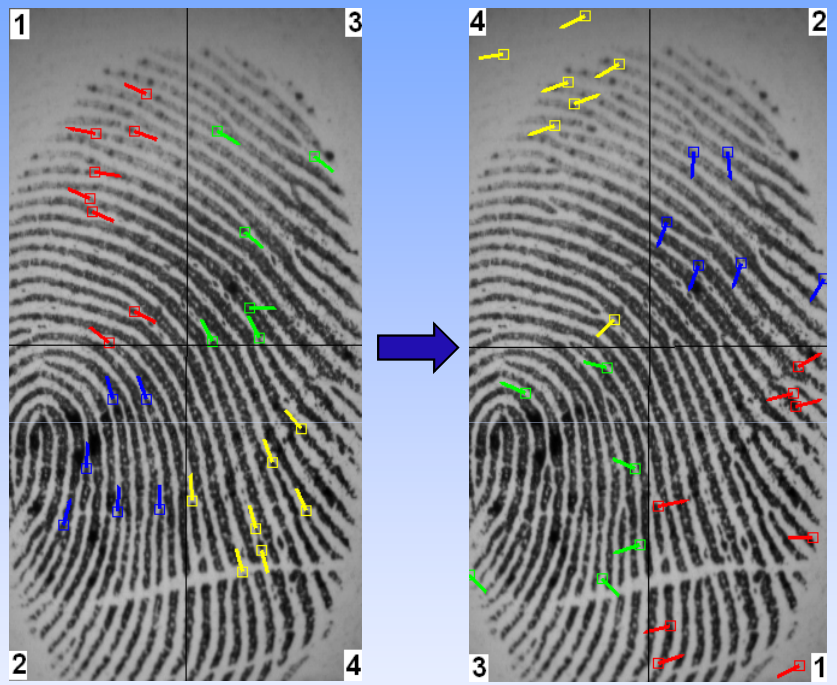
Biometric Feature Adaptations

Modality - Feature	Approach	Representation	
		Original	Final
Fingerprint - minutiae (Nagar et al., Xu et al., Farooq et al., Cappelli et al.)	Local aggregates, spectral minutiae, triplet histogram, cylinder-code	Point set	Binary string
Fingerprint - minutiae (Sutcu et al.)	Geometric transformation	Point set	Quantized vector
Fingerprint - orientation field & Gabor features (Bringer et al.)	Reliable component selection & quantization based on statistical analysis of features	Real vector	Binary string
3D Face – local curvature (Kelkboom et al.)			
Face - Gabor features (Kevenaar et al.)			
Face – PCA/LDA (Feng and Yuen)	Division into stable integer & unstable real parts	Real vector	Quantized vector
Iris – Iriscode (Nandakumar and Jain)	Salting/fuzzy commitment of different bit segments	Binary string	Point set

Which scheme gives the most compact & discriminable representation?

Hardened Fuzzy Vault

- Salting + fuzzy vault to introduce revocability
- Transform each fingerprint quadrant using password
- Increase uniformity of minutiae distribution



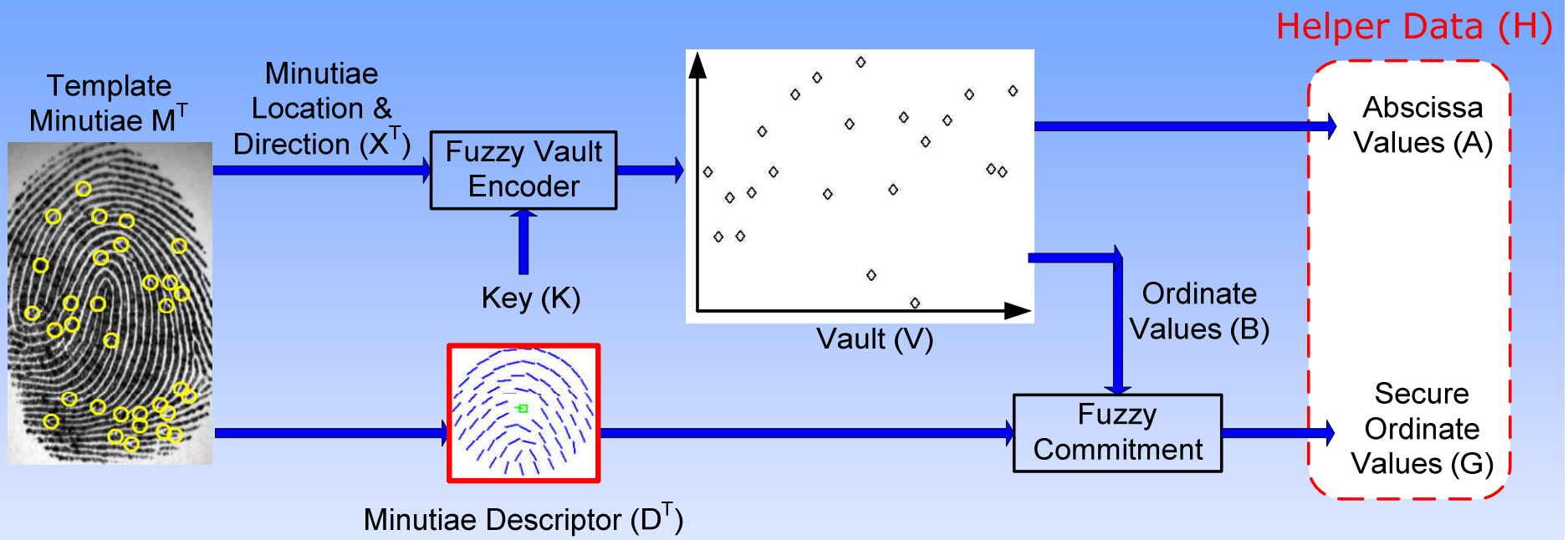
Original Template

Transformed Template

As secure as original vault even if password is compromised

Nandakumar, Nagar and Jain, Hardening Fingerprint-based Fuzzy Vault Using Password, ICB 2007

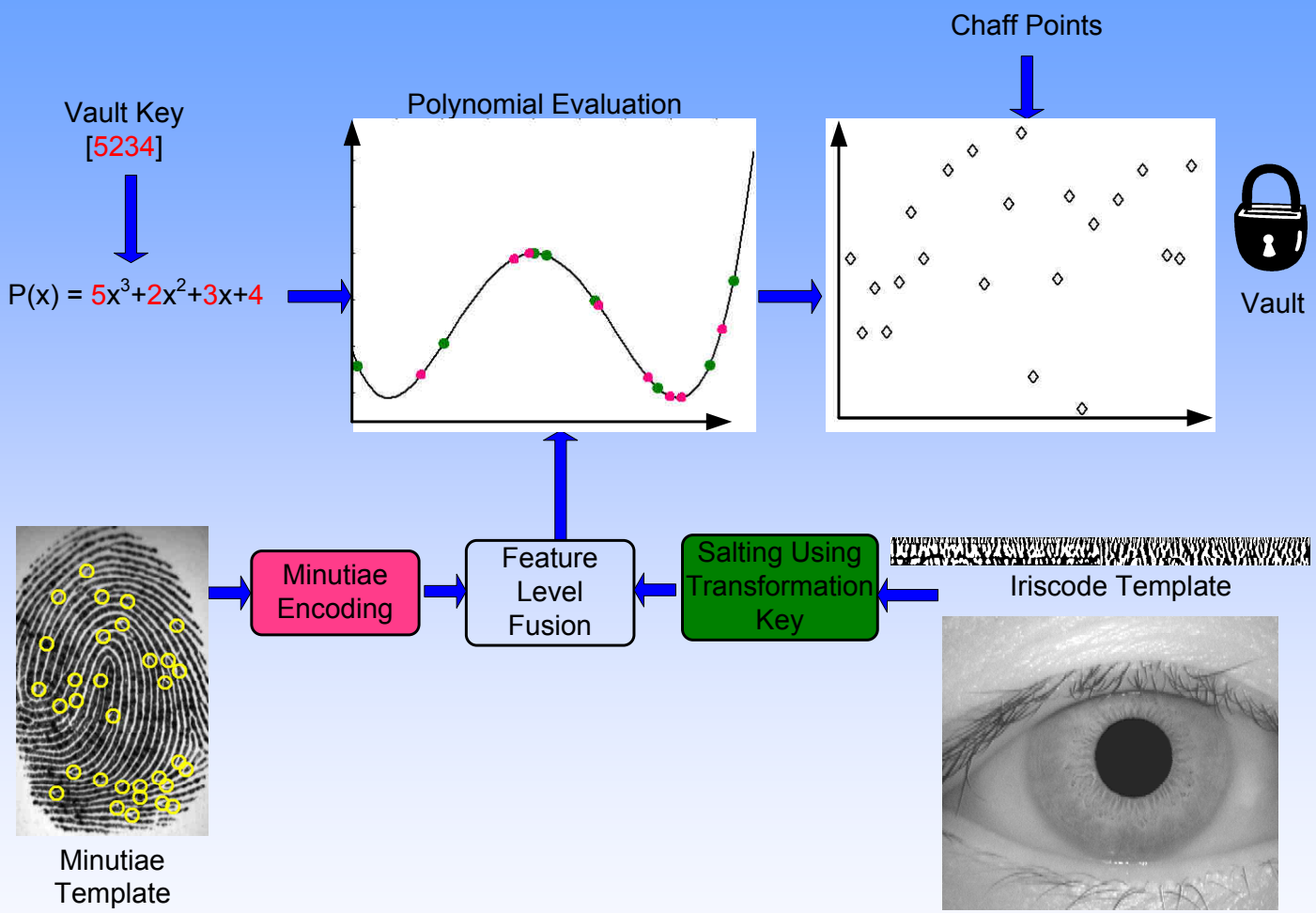
Vault with Minutiae Descriptors



Local minutiae descriptors are bound to the ordinate values of the vault using fuzzy commitment; improves matching performance and security

Nagar, Nandakumar and Jain "Securing Fingerprint Template: Fuzzy Vault with Minutiae Descriptors", Proc. ICPR, 2008

Multibiometric Fuzzy Vault



Iriscode is transformed into point set using fuzzy commitment & combined with minutiae to improve both the matching performance and vault security

Nandakumar and Jain, "Multibiometric Template Security Using Fuzzy Vault", BTAS 2008

Template Security Evaluation

- How difficulty it is to recover the original template from the stored template (brute-force attack)?
- Typically expressed in bits & measured based on
  - Avg. no. of trials needed to recover the template
  - Entropy of original template given the secure sketch
- Estimate of security requires a model of the biometric feature distributions
- Zero-effort attacks (FAR) is reported separately

Security of Cryptosystems

- Fuzzy vault[1]

$$\text{Security} = \log_2\left(\frac{C(r,n+1)}{C(t,n+1)}\right)$$

r: total no. of points in the vault
t: no. of genuine points
n: degree of polynomial used

Assumption: Both genuine and chaff points are uniformly distributed

- Fuzzy commitment[2]

$$\text{Security} \approx \log_2\left(\frac{2^I}{C(I,\rho I)}\right)$$

I: Entropy of binary template
ρ: Fraction of errors corrected

Assumption: Reliable estimate of entropy (no. of i.i.d bits) is available

How to modify features to satisfy these assumptions?

[1] Nandakumar, Jain and Pankanti, "Fingerprint-based Fuzzy Vault: Implementation and Performance", *IEEE Transactions on Info Forensics & Security*, 2007

[2] Hao, Anderson, and Daugman, "Combining Crypto with Biometrics Effectively," *IEEE Trans. Computers*, 2006

Comparison of Fingerprint Cryptosystems

Approach	FNMR at Zero-FMR*	Security
Fingerprint fuzzy vault*	14%	$\frac{C(224,11)}{C(24,11)}$ = 39 bits
Fuzzy commitment based on BiPS*	6%	$\frac{2^{327}}{C(327,98)}$ = 43 bits
Hardened fuzzy vault with password*	<10%	$\frac{C(224,8)}{C(24,8)}+18(password)$ =45 bits
Fuzzy vault with minutiae descriptor*	7%	$\frac{C(224,9)}{C(24,9)}+18(descriptor)$ =49 bits
Best matcher in FVC2002	0.3%	N.A.
Fuzzy vault with two fingers#	12.5%	$\frac{C(672,12)}{C(72,12)}$ = 40 bits
Fuzzy vault with multiple biometrics (fingerprint + iris)#	1.8%	$\frac{C(884,14)}{C(84,14)}$ = 49 bits

* FVC2002-DB2; 100 genuine matches and 9,900 (4,950 independent) impostor matches

Fingerprint – MSU-DBI database (160 users); Iris – CASIA v1.0 (108 users)

Security (guessing entropy) of 8 character password is ~18 bits[1]

[1] Burr et al., Electronic Authentication Guideline, NIST Special Publication 800-63, 2006

Summary

- Biometrics is essential for trusted identification, but we need tamper proof systems with low error rates
- Template security is an important issue because compromised templates cannot be revoked/reissued
- A template protection scheme with provable security & acceptable performance has remained evasive
- Challenge is to design cryptosystems that
  - generate non-linkable templates
  - provide good trade-off between accuracy & security
  - utilize feature adaptation schemes that preserve accuracy and allow easy fusion of modalities

Additional References

[1] Albert Bodo, “Method for producing a digital signature with aid of a biometric feature,” German patent DE 42 43 908 A1, (1994)
[2] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy and B.V.K. Vijaya Kumar, "Biometric encryption using image processing," Proc. of SPIE, vol. 3314, 178-188, 1998
[3] Ari Juels and Madhu Sudan, \A fuzzy vault scheme", Proceedings of the IEEE International Symposium on Information Theory, A. Lapidoth and E. Teletar, Eds., page 408, Lausanne, Switzerland, 30 June - 5 July, 2002.
[4] A. Juels and M. Wattenberg, “A fuzzy commitment scheme,” in Proc. 6th ACM Conf. Computer and communications Security,G. Tsudik, Ed., pp. 28–3, 1999
[5] Sharat Chikkerur, Alexander N. Cartwright, Venu Govindaraju: K-plet and Coupled BFS: A Graph Based Fingerprint Representation and Matching Algorithm. ICB 2006:
[6] Jeffers, J., Arakala, A.: Minutiae-based Structures for a Fuzzy Vault. In: Proc. of. 2006 Biometrics Symposium, MD, USA, September 19-21, 2006 (2006)
[7] T. E. Boult, W. J. Scheirer, and R. Woodworth, “Revocable Fingerprint Biotokens: Accuracy and SecurityAnalysis,” in IEEE Conference on Computer Vision andPattern Recognition, June 2007, pp. 1–8.
[8] J. Feng. Combining minutiae descriptors for fingerprintmatching. Pattern Recognition, 41(1):342–352, 2008.
[9] Raffaele Cappelli, Matteo Ferrara, and Davide Maltoni. Minutia cylinder-code: a new representation and matching technique for fingerprint recognition. IEEE Transactions on Pattern Analysis And Machine Intelligence, 2010.
[10] A. K. Jain, A. Ross, and S. Prabhakar, "Fingerprint Matching Using Minutiae and Texture Features", Proc. I nternational Conference on Image Processing (ICIP), pp. 282-285, Greece, October 7-10, 2001.
[11] A. K. Jain, S. Prabhakar, L. Hong and S. Pankanti, "FingerCode: A Filterbank for Fingerprint Representation and Matching", Proc. IEEE Conference on CVPR, Colorado, Vol. 2, pp. 187-193, June 23-25, 1999.
[12] Aglika Gyaourova, Arun Ross: A Novel Coding Scheme for Indexing Fingerprint Patterns. SSPR/SPR 2008: 755-764
[13] J. Bringer and V. Despiegel, Binary Feature Vector Fingerprint Representation From Minutiae Vicinities, BTAS, 2010
[14] Xu, H. and Veldhuis, R.N.J. (2010) Binary Representations of Fingerprint Spectral Minutiae Features. In: 20th International Conference on Pattern Recognition (ICPR 2010), 23-26 August 2010, Istanbul, Turkey. 1212-1216
[15] Nagar, A.; Rane, S.D.; Vetro, A., "Alignment and Bit Extraction for Secure Fingerprint Biometrics", SPIE Conference on Electronic Imaging, Vol. 7541, 75410N , January 2010
[16] Yagiz Sutcu, Qiming Li, Nasir D. Memon: Secure Biometric Templates from Fingerprint-Face Features. CVPR 2007
[17] F. Farooq, R. M. Bolle, T.-Y. Jea, and N. Ratha, “Anonymousand Revocable Fingerprint Recognition,” in Proc. ComputerVision and Pattern Recognition, Minneapolis, June 2007.