(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
3 October 2002 (03.10.2002)

PCT

(10) International Publication Number
WO 02/078249 A1

(51) International Patent Classification[7]: H04L 9/32

(21) International Application Number: PCT/SG01/00051

(22) International Filing Date: 23 March 2001 (23.03.2001)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **KENT RIDGE DIGITAL LABS** [SG/SG]; 21, Heng Mui Keng Terra, Singapore 119613 (SG).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **WU, Yong, Dong** [CN/CN]; Block 10, Ghim Moh Road, #13-80, Singapore 270010 (CN).

(74) Agent: **GREENE-KELLY, James, Patrick**; Lloyd Wise, Tanjong Pagar, P.O. Box 363, Singapore 910816 (SG).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

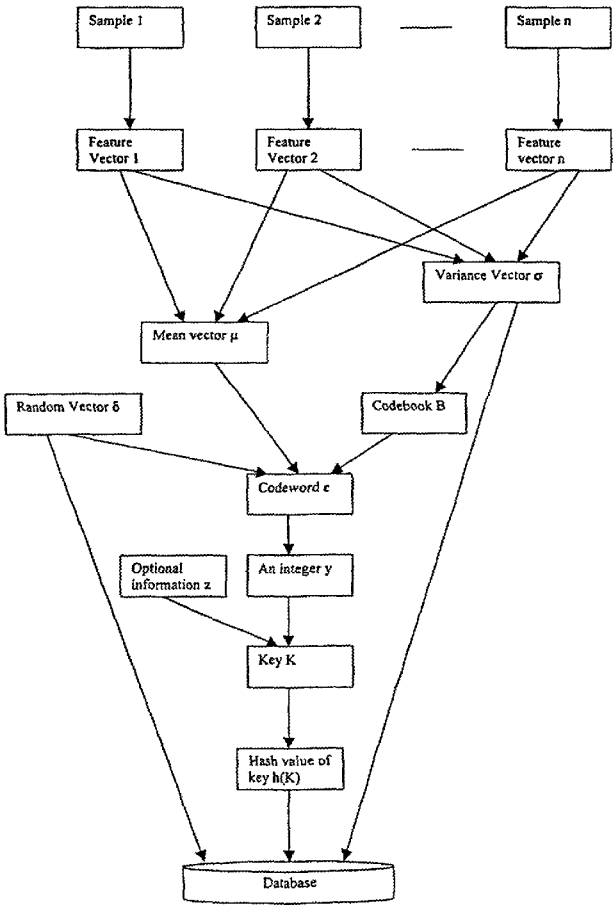
(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report*

[Continued on next page]

(54) **Title:** METHOD OF USING BIOMETRIC INFORMATION FOR SECRET GENERATION



(57) **Abstract:** A method and system that generates a secret from individual's biometric information, such as voice, handwriting and fingeprint. It extracts a feature vector from the captured biometric data. The feature vector is then transformed into a codewood, and the codeword is used to construct the secret. A one-way hash of the secret is stored. Only if a user generates a new secret that has the same hash value as that stored will the user be confirmed. To keep pace with the gradual change of the measured biometric features, the secret can be updated adaptively. The secret may be an encryption key.

WO 02/078249 A1

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.