ISSN 1991- 8690 الترقيم الدولي 8690 - 1991

Website: http://jsci.utq.edu.iq Email: utjsci@utq.edu.iq

# Cryptographic key Generation Using Fingerprint Biometrics

Huda Ameer Zaki

Computer Science Department ـ Shatt Al-Arab College University ـBasrah / Iraq

Email: hazz79@yahoo.com

## Abstract

At the present time progress of communications technologies has resulted to post large amounts of digital data in the media shared among the people, this has necessitated the development of cryptographic techniques to be one of the building blocks for the security of the computer, so that became the encryption feature increasingly important to the security of the computer. This paper proposed a method for generating a key using fingerprint features to ensure the security of the system against hackers. This technical consists of two parts the first is the EPROM memory filled with information of fingerprint after processed by the enhancement, binarization and thinning operations and then 512 numeric values has been extracted. The second part is a set of linear shift registers where every movement for system registers is an address in the memory where the dimensions of memory (8x64), the first three registers give the row address while the registers ordered by two to seven give the column address of EPROM array. The strength of the chain of random numbers which produced by making originating from two different worlds linked to the same user, is a goal makes this technique useful for several uses, such as using output as encryption keys, or use it as a digital series for personal definition for security systems.

**Keywords:** Fingerprint, Cryptography, Binarization, Thinning, Morphological Operations, Minutiae Points.

# توليد مفتاح تشفير باستخدام القياسات الحيوية لبصمة الأصبع

هدى أمير زكي

قسم علوم الحاسبات ـ كلية شط العرب ـ جامعة البصرة \ العراق

## الخلاصة

لقد أدى التقدم في تكنولوجيا الاتصالات في الوقت الحاضر لنشر كمية كبيرة من البيانات الرقمية في وسائل الاتصال المشتركة بين الناس. وهذا الأمر استلزم تطوير تقنيات تشفير لتكون واحدة من اللبنات الأساسية لأمن وحماية الحاسوب. اقترح هذا البحث طريقة توليد مفتاح باستخدام ميزات بصمة الإصبع لضمان امن النظام ضد المتسللين الذين يحاولون اختراق الأنظمة وقرصنة المعلومات. تتكون هذه التقنية من جزئين، الأول هو ذاكرة تملئ بالمعلومات من البصمة بعد مرورها بعمليات تحسين لصورة البصمة ومن ثم استخلاص 512 قيمة رقمية. والجزء الثاني يتضمن مجموعة من مسجلات إزاحة خطية حيث تمثل كل حركة لمنظومة مسجلات الإزاحة عنوان في الذاكرة والتي أبعادها (64X8)، المسجلات الثلاثة الأولى تعطي عنوان الصف في الذاكرة، أما المسجلات من الثاني إلى السابع تعطي عنوان العمود في الذاكرة التي تخزن قيمة رقمية للبصمة. إن قوة سلسلة الأرقام العشوائية المنتجة من مصدرين مختلفين مرتبطين بنفس المستخدم كالبصمة وكلمة السر هدف يجعل لهذه التقنية عدة استخدامات، كاستخدام المخرجات كمفاتيح تشفير، أو استخدامها كسلسلة رقمية للتعريف الشخصي بالأنظمة الأمنية.

## 1. Introduction

Information security today is becoming more and more important. Cryptography is an important feature of computer and network security. Many cryptographic algorithms are available for securing information e.g. RSA, DES, AES etc. Normally using cryptosystem has a number of associated inconveniences and problems such as [1]

- Conventional Cryptography authenticates messages based on the key but not on the user. Hence unable to differentiate between the legitimate user & an attacker.
- These keys can be guessed or cracked.
- Large size of strong keys results in longer delay in encryption/decryption.
- It is difficult to remember the keys, storing them in a data base may be insecure.
- Moreover, maintaining and sharing lengthy, random keys is the critical problem in the cryptography system.

Using biometrics by means of cryptography is a new hot research topic, Biometrics and cryptography are two potentially complementary security technologies. Biometrics is defined as any individual on the basis of physiological and behavioral characteristics, that the most common physiological features include face, fingerprint, hand, ear, iris, and DNA while the most common behavioral features include talking, walking, and signature [2].A good biometric is characterized by use of a feature that is highly unique, so that the chance of any two people having the same characteristic will be minimal, so that the feature does not change over time, and be easily acquired in order to provide convenience to the user, and prevent misrepresentation of the feature. Fingerprint recognition is the oldest method of biometric identification [3].Many papers have been published in the field of key generation using fingerprint biometric, Dr. R. Seshadri et al. described a biometric-crypto System generates an encryption key from fingerprints for calculating the MAC value of the information. Password can penetrate through trial and error, but the system remains based on biometrics difficult to break [4]. M. S. Altarawneh et al. have introduced an approach to generate encryption key from fingerprint sample. The idea is based on slicing window partitioning the area of extracted minutiae, using the Euclidean distance between detected core point and extracted minutiae points then vector generation used to derive a biometric key that can be used to encrypt a plain text message and its header information [5]. C. Nandini et.al presented a unique technique for generation of cryptographic key; the authors have used hashing technique in the finger trivia using completely different set of symmetric hash function for various users that is both secured and fast. k-plets has been extracted from each fingerprint image and calculate the hash values based on the nearest neighbors of a minutia point in the k-plet. A combination of these hash values are used to generate a key. This key can be used for any type of cryptography. The generated key was tested using existing AES algorithm with 128 bits key size and increase within the security was theoretically proved [6]. Lee et al proposed an approach to provide both the automatic alignment of fingerprint data and higher security by using a 3D geometric hash table. Based on the experimental results the proposed approach confirmed that the using of 3D geometric hash table with the idea of the *fuzzy vault* can perform the fingerprint verification securely even with one thousand chaff data included [7].In this paper, a fingerprint biometric is used for generating the encryption key using this technical consists of two parts the first is the EPROM memory with dimensions (8x64) filled with extracted 512 numeric information of fingerprint. The second part is a set of linear shift registers which each number shifted by shift register represented the address in memory where every movement system registers displacement address in the memory.

## 2. The Comprehensive Structure of Cryptography Key Generation

Biometric cryptosystems combines both biometrics and cryptography to afford the advantages of both for security purposes. This technique provide the advantages like better security levels for data transmission and eliminating the must to memorize passwords or to carry tokens etc. In my approach for generating cryptographic key fingerprint has been selected as the biometrics feature. Minutiae points have been extracted from the fingerprint and that points set are used for generating cryptographic key. Several steps have been achieved in order to generating cryptographic key from fingerprint biometric as follow: The conceptual diagram of the proposed approach is illustrated in Figure 1.

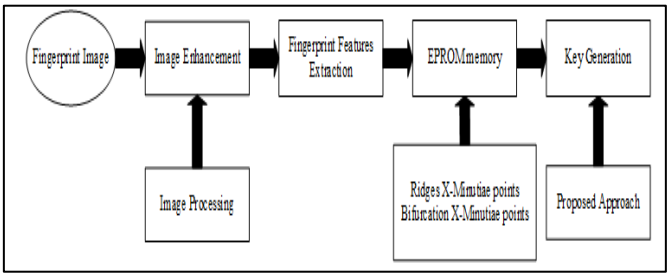


Figure 1: Key generation process

## 3.Methodology

### A.Fingerprint characteristics

Fingerprints have been used for more than a century, as it represents the most widely used technology for biometric identification and to the fact that a fingerprints are formed in the fetal stage and remain structurally unchanged throughout an individual's lifetime. There are two factors affecting the high ratio of identification named as speed and reliably of minutiae extraction from the input fingerprint image. Minutiae points are local ridge characteristics that occur either at a ridge ending or bifurcation. A ridge ending are the points where the ridge curve terminates and the bifurcations are where a ridge splits from a single path to two paths at a Y-junction. Figure 2 shows an example of a ridge ending and a bifurcation [8].

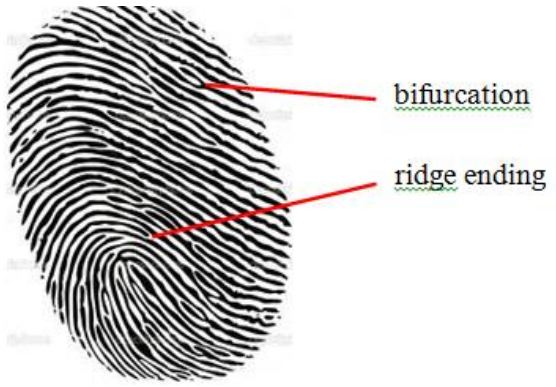


Figure 2: Fingerprint Image with different identifying points

### B.Fingerprint Minutiae extraction

- **Image Enhancement:** The main reasons of performing image enhancement are to improve the contrast between ridges and valleys and reduce noises in the fingerprint image and protect the true configuration of them. The enhancement method is the modification of image brightness, contrast, and equalization.
- **Binarization:** It is the process that converting a grey scale image into a binary image. An adaptive binarization algorithm has been used for high accuracy conversion. In this case there is no universal threshold value of whole image, but for each pixel its own threshold value is calculated separately depending on pixel location which the average value of intensity of neighborhood pixels block has been represented as threshold value. If the gray value of the pixel is greater than threshold, then it is set to white, otherwise it is black. This method is much more accurate, if the size of neighborhood pixels block for threshold calculation is selected appropriately. Analyses have shown that the optimum size of pixels block depending on fingerprint image. The best results are obtained when block size is a little bigger than twice of the thickness of the ridge.
- **MorphologicalOperations:** Morphological opening and closing on the binary image by using structuring element has been performed. The structuring element is a single structuring element object, as opposed to an array of objects for both open and close. Then as the result this approach throws away those leftmost, rightmost, uppermost and bottommost blocks out of the bound so as to get the tightly bounded region just containing the bound and inner area.
- **Thinning:** Before the minutiae extraction stage, a thinning process is used to on skeletonize the binary image by reducing all lines to a single pixel thickness.
- **Minutiae Extraction:** The Crossing Number (CN) method is used to perform minutiae extraction effectively. This method extracts the ridge endings and bifurcations from the skeleton image by examining the local neighborhood of each ridge pixel using a 3X3 window.

### C.Key generation based on random generation system

The proposed random number generator system for personal identification consists of two steps. At first step, the information of fingerprint minutiae that represented by Ridges-X and Bifurcations-X are stored in 512 bit EPROM memory which the memory is represented by 8 x 64 array while in the second step the eight registers have been used which length of each register (11,13,9,13,11,17,13,17) respectively, these registers have been filled by key of eight letters. The bits of ASCII code of each letter have been distributed in the eight registers as shown in Figure 3.

The eight registers give an address of a certain row of the EPROM memory by the following steps:

- The passwords letters converts to ASCII code which each bit of ASCII code number puts in each register vertically.
- The eight registers will be shifted by selected number of times.
- The bits of each first three registers have been concatenated in order to generate number uses as row address of EPROM array.

- The number represented by six bits started from bit number two of each register uses as column of EPROM array.
- The numbers of EPROM array which indicated by rows and columns have been concatenated to generate key as shown in Figure 3.

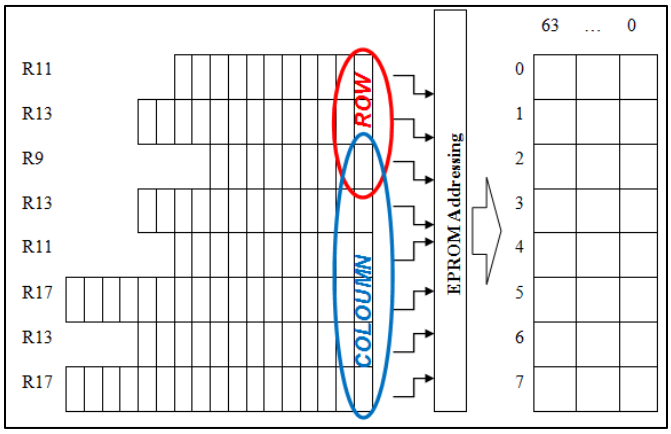


Figure 3: Block diagram of proposed key generator method

## 5.Experimental Result

The proposed approach is implemented by MATLAB which nine samples of fingerprint image have been selected form The Third International Fingerprint Verification Competition (FVC2004) database. These samples have been used to generate keys, which successfully tested as shown in Table 1.
First step is the fingerprint samples have been enhanced and then minutiae of them have been extracted as shown in Figure 4

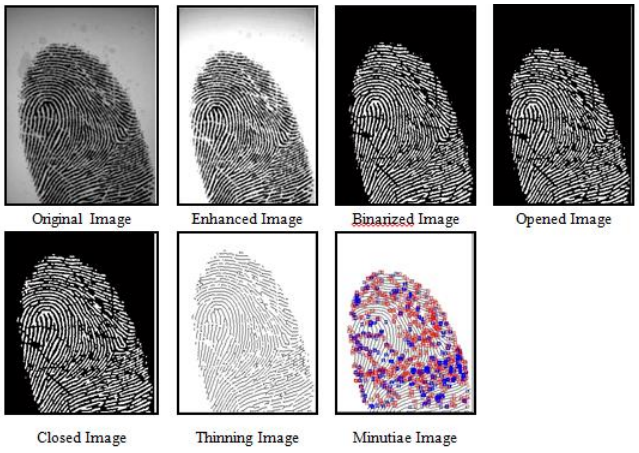


Figure 4. After image processed by image processing algorithm

the second step, the extracted fingerprint minutiae represented by Ridges is as follow

F1 = 213 205 230 234 224 176 158 215 256 260 172 164 179 229 249 156 186 288 234 149 155 160 229 184 188 155 302 252 318 136 148 319 130 237 252 131 160 223 307 226 236 157 299 146 184 252 291 284 319 245 135 300 306 331 182 221 225 302 331 341 135 294 129 185 261 351 159 250 153 250 362 307 128 159 221 305 120 122 224 264 316 126 252 115 152 175 196 366 121 193 100 101 219 307 269 303 144 176 261 305 220 224 257 300 266 100 145 193 257 151 276 169 306 359 97 117 138 273 203 133 303 169 298 91 110 116 221 282 93 280 122 150 314 324 97 111 299 302 105 150 321 333 121 223 309 283 352 129 223 350 186 188 317 313 301 103 111 129 188 297 322 133 87 219 363 105 222 294 360 291 111 135 302 319 369 87 298 367 326 152 135 295 324 227 230 293 134 152 331 141 300 242 245 298 154 328 143 335 351 370 155 301 310 368 100 168 249 334

Which F1 is Ridge-X of the minutiae points. The password has been selected is (MINUTIAE) which is converted to ASCII code and stored in eight registers where the first cell filled with 1 in all of them to avoid the zero value as follows:

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| R11 | | | | | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 1 |
| R13 | | | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 |
| R9 | | | | | | | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 1 |
| R13 | | | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 1 |
| R11 | | | | | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 |
| R17 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| R131 | | | | | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| R17 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |

Finally, eight registers have been shifted 100 times and then rows and columns of EPROM array is found to generate Key

Generated Key = 153 152 145 190 157 149 332 150 249 129 184 111 234 234 188 352 153 185 367 369 342 234 231 188 156 229 234 367 249 291 318 141 135 363 138 87 245 306 199 136 133 219 314 331 229 341 213 245 297 121 216 111 297 149 318 135 321 93 242 227 87 294 297 230 333 135 213 330 210 234 233 185 321 234 149 93 369 111 135 135 280 179 252 319 149 300 178 156 219 205 248 135 291 150 87 122 248 111 223 326

Table 1: Samples of fingerprints and their generated keys

| Fingerprint | Password | Generated Key |
|---|---|---|
|  | COPYBOOK | 295 181 247 157 256 164 63 164 247 217 237 85 325 302 166 322 192 96 85 99 268 48 125 165 130 196 86 82 205 86 134 181 48 88 281 231 89 134 185 192 264 148 292 229 185 288 299 86 49 189 324 125 146 322 203 258 255 207 299 82 205 50 229 255 48 92 322 49 145 253 246 157 96 92 166 208 89 217 198 211 247 124 208 125 198 283 49 119 267 293 170 326 208 82 164 217 262 130 216 |
|  | SECURITY | 104 326 251 224 104 138 64 96 251 156 290 251 175 167 329 292 211 108 329 167 306 162 192 138 297 108 234 68 251 251 282 193 95 309 49 148 200 75 118 167 50 235 246 253 294 169 297 172 75 327 275 251 214 172 287 297 148 138 327 292 253 268 156 234 49 179 114 329 127 238 170 97 327 319 167 251 54 91 234 83 95 224 179 204 306 217 162 156 319 167 229 297 75 78 253 64 327 315 159 |
|  | OPTIMIST | 194 267 161 288 68 267 272 224 265 175 297 239 329 246 89 175 285 244 275 288 199 307 180 224 259 298 161 309 321 321 119 116 161 58 82 89 68 161 285 248 272 116 175 111 235 94 116 128 280 321 136 238 95 292 100 94 175 295 131 140 139 192 175 328 283 272 246 52 175 259 202 321 69 243 198 275 316 265 89 89 287 246 312 20 246 246 324 175 161 259 89 94 299 288 253 324 272 82 52 |
|  | PLANNING | 470 277 166 471 501 471 240 275 397 219 190 248 223 144 158 172 501 406 275 225 175 360 438 301 211 416 302 402 314 350 182 333 344 321 310 211 353 316 404 530 168 158 113 148 205 281 211 257 356 185 364 223 118 360 172 330 160 106 530 353 310 212 379 114 226 257 184 427 356 196 471 185 225 310 109 294 226 448 242 386 223 330 257 248 248 98 106 205 214 223 316 198 88 193 399 133 188 288 |
|  | ACADEMIC | 269 152 328 76 130 433 243 215 510 63 244 414 146 121 202 237 71 392 315 506 271 256 63 120 356 243 480 47 125 463 480 436 271 486 71 375 33 219 244 255 499 522 52 433 234 262 518 196 419 493 494 494 375 13 405 71 237 215 207 237 309 496 405 518 499 126 376 139 333 320 144 509 493 269 234 333 408 262 271 221 264 47 37 367 279 113 244 33 414 429 59 221 376 419 61 144 375 522 245 42 |
|  | COMMERCE | 117 277 330 363 330 344 292 261 261 275 226 174 395 121 114 52 118 116 491 266 371 177 78 350 113 103 104 100 103 455 330 276 122 331 396 461 313 113 234 371 147 297 279 146 125 313 335 124 279 297 455 49 461 444 462 105 491 303 118 315 350 113 212 371 203 291 396 52 93 114 196 313 171 117 371 461 455 261 375 337 462 103 114 494 315 375 396 444 |
|  | MOVEMENT | 87 525 234 392 151 358 129 470 286 445 302 330 344 454 394 330 165 196 461 292 241 549 241 87 129 123 146 531 85 525 196 196 454 273 426 115 172 215 306 526 507 110 375 132 300 159 328 210 461 461 507 196 506 313 268 389 510 198 114 196 198 277 525 520 302 226 128 379 385 85 305 132 450 510 210 196 302 375 226 390 479 226 412 375 243 80 330 87 280 391 313 273 114 389 146 123 202 273 |

## 6. Conclusion

In this paper, proposed approach has been presented that generates cryptographic key from fingerprint images in an efficient manner. The approach takes advantage of computer processing speeds, biometric data, and standard encryption algorithms to provide a novel way of generating cipher keys without having to remember complicated sequences which might be lost, stolen, or even guessed. This approach is simple and easy to implement also difficult to crack Key generated by this approach because random generation method is used to generate Key.

## Refrences


[1] Rashi Bais, K.K.Mehta, " Biometric Parameter Based Cryptographic Key Generation", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-5, June 2012

[2] Qinghai Gao, " Error Tolerance Techniques For Binding Cryptographic Key With Biometrics", Department of Security Systems, Farmingdale State College, SUNY ,2350 Broadhollow Road, Farmingdale, NY 11735

[3] Manish Manoria, Ajit Kumar Shrivastava, Satyendra Singh Thakur, DebuSinha, "Exploring the Prospect of Secure BiometricCryptosystem using RSA for BlindAuthentication", International Journal of Wisdom Based Computing, Vol. 1 (2), pp. 24-27, August 2011.

[4] R.Seshadri and T.Raghu Trivedi, "Generate a key for MAC Algorithm using Biometric Fingerprint", International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC), Vol.1, No.4, December 2010.

[5] M.S. Altarawneh, L.C. Khor, W.L. Woo, and S.S. Dlay, "Crypto Key Generation Using Slicing Window Algorithm",

[6] C. Nandini and B. Shylaja., "Efficient Cryptographic key Generation from Fingerprint using Symmetric Hash Functions", International Journal of Research and Reviews in Computer Science (IJRRCS) Vol. 2, No. 4, ISSN: 2079-2557, August 2011.

[7] S. Lee, D. Moon, S. Jung, and Y. Chung, " Protecting Secret Keys with Fuzzy Fingerprint Vault Based on a 3D Geometric Hash Table", presented at ICANNGA
2007, Warsaw, Poland, 2007.

[8] Sasan Golabi, Saiid Saadat, Mohammad Sadegh Helfroush, and Ashkan Tashk, "A Novel Thinning Algorithm with Fingerprint Minutiae Extraction Capability" , International Journal of Computer Theory and Engineering, Vol. 4, No. 4, August 2012