A Compressed & Secure Multimodal Biometric System for Palm Print & Facial Image

Nidhi Verma[1] Deepak Agrawal[2]
[1,2]Department of Computer Science & Engineering
[1,2]Takshshila Institute of Engineering & Technology, Jabalpur M. P., Pin- 482001, India

Abstract— Increase of computing has result in associate degree explosion within the volume of data to be saved on magnetic disk and send over the net. This enlargement has result in a requirement for knowledge compression that is that the ability to scale backs the number of or Internet-Bandwidth needed managing this data. Authentication systems area unit ready to be supported passwords, security tokens, biometric, or mixtures of them. Passwords area unit words, phrases, or alpha-numerical (PINs) that function short kind indicators of a personnel identity. {They area unit| they're} typically shaped by approved users throughout the enrolment or registration part adore making mortal accounts and are reserved secret from others. The Authentication method involves corroboratory the identity of a personal claim access to 1 or additional resources of a system. My paper gives a review of fusion and compression of knowledge techniques.

Key words: Compression, Magnetic Disk, Bandwidth, PIN, Registration

I. INTRODUCTION

A person will apprehend the entire issue reminiscent of passwords, Personal Id. range (PIN) and any specific range; however they're usually used commercially to ascertain the distinction of associates and enemy (2). At this time on a daily basis the duty of recognizing person isn't any longer restricted to human. There exist some ways to acknowledge oneself acknowledgement (3). As a member of this procedure of progression we tend to ever additional usually ought to verify our identity to technological systems (4, 5).

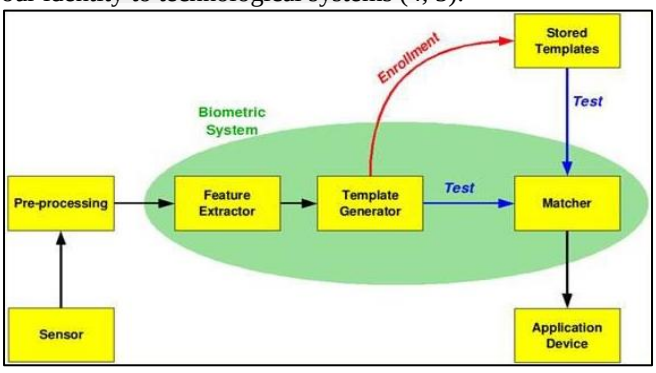

Fig. 1: Detection by Biometric Uniqueness

A biometric characteristic be faultless if it fulfills all these criterions. Particularly due to chronological variations of dynamic characteristics, & comparatively straightforward chances to reproduce them, static characteristics look like appropriate for a biometric recognition method. Biometric technique may be defined by an automated method to distinguish or authenticate the ID of an alive person on the basis of his physical quality or behavioral quality (10). The effectiveness is determined according to various fundamental rates that for example specify the no. of correct or incorrect acknowledged personnel. Therefore, mainly significant rates are given below (5)

A. *FMR (False Match Rate)*

It indicates the rate (in percent) of by mistake accepted personnel.

B. *FNMR (False Non-Match Rate)*

It indicates the rate (in percent) of by mistake non-accepted personnel (7).

II. BIOMETRIC CHARACTERISTICS

The method is often creative & typically easier than would be estimated. One question newcomer to the ground asks over is what regarding a latex finger, prosthetic eye and digital acoustic tape etc. Biometric personal authentication may be finding out by physiological characteristics that distinguish one person from another. Some physiological characteristics used for automatic biometric authentication are as follows:

- Hand-geometry,
- Face,
- Retina,
- Iris,
- Hand veins.
- Fingerprint,
- Palm-print,
- DNA

A. *Storing the Creature*

For the duration of the feature gathering procedure at least 1 physical or behavioral point is captured by a skilled sensor (7, 9). The obtained raw image may either be used directly, or an optional feature extraction and template generation takes place depends on further use (4).

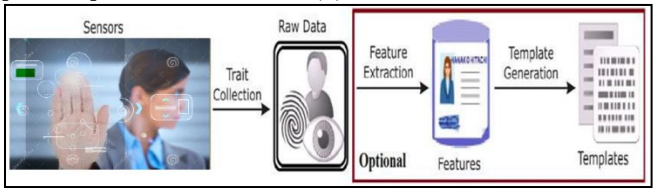

Fig. 2: Creature collection & pattern creation

B. *Enrollment Listing*

It covers the primary feature grouping on one hand and storage of the captured data on the other hand (10). To registering an enrollment is the mainly essential procedure of the biometric detection.

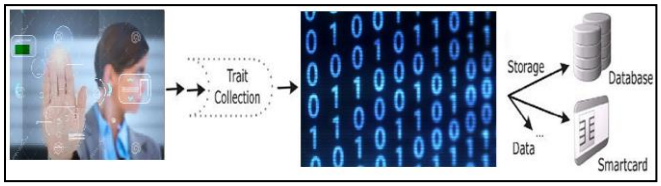

Fig. 3: Enrollment Listing: the Enrolled Creatures are Stored

C. Verify the Person

Verification is the 1 by 1 process which can biometric information presented by an individual (live template) with biometric information saved in database (user's template). The templates of user selected by the user's ID or PIN.

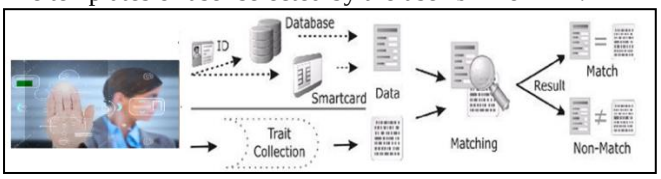

Fig. 4: Matching System

Thus verification can be treated as combination of authentication mode that who (client) knows or possesses (password, PIN or ID) and biometric features. For instance if the user possesses a smartcard on which the reference feature is stored, he could provide it directly to the system (10).

Hence for the higher security multi issue authentication is best, so parole with anybody biometric system build the virtual banking with higher security in forth returning years.

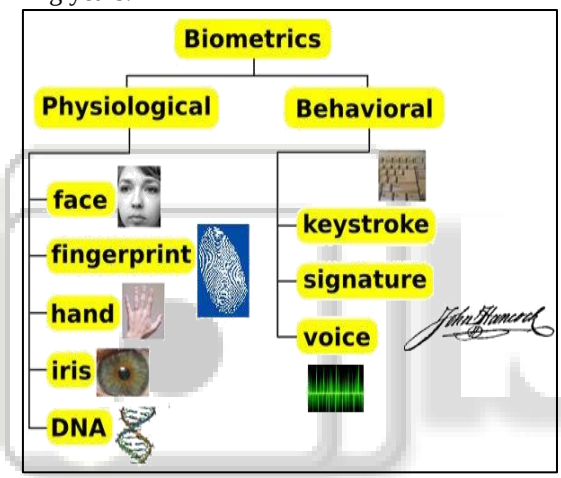

Fig. 5: Biometrics Classifications

III. HAND-GEOMETRY BIOMETRICS

These options are beneath development by many firms, together with Bio Met Partners, Pal metrics, and BTG. The company itself does not sell any end-user configured products. The Bio Met strategy, for its two-finger Digi-2 scanner is interesting. The company only supplies OEM components to partners for integration into attendance and control ATMs and other equipment. Hand pure mathematics is that the folks of biometric systems. vi totally different hand scanning product developed over this era tally the foremost commercially prosperous biometric to this point, the ID-3D Hand key from Recognition Systems. The Hand key appearance at each the highest and facet views employing a inbuilt video camera and compression algorithms.

Fig. 6: Hands Scanning Biometric Process

IV. FACIAL RECOGNITION

Now the scientists use neural either network technology or applied mathematics correlation of the face's geometric form. Biometric identification and verification is that the quickest growing space currently on a daily basis. Most of those efforts square measure stirred up by the quick rise in multimedia system video technology that's introduction cameras within the work, and eventually the house.

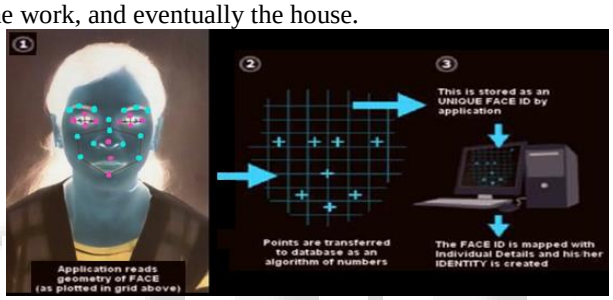

Fig. 7: Facial Recognition Process

More specific applications comparable to screening welfare info for duplicates and flying field lounges for terrorists should advance with time (11). Still, interest from government agencies and even the financial sector is high, stimulating the development hard work however developers. Given this pace of development, it is probable that our multimedia PC will recognize us via a camera built into our monitor for teleconferencing on the electronic superhighway.

V. PROPOSED WORK

A. Types of Multi-Biometric Systems

Multi-biometric systems can be categorized by considering the way you are taking multiple sources of evidence. There can be different options to have sources of evidence. Consideration can be made for multiple instances, multiple algorithms, multiple sensors or sometime multiple traits. Based on this, we can categorize multi-biometric systems in following categories:

1) Multi-sensor systems
2) Multi-algorithm systems
3) Multi-instance systems
4) Multi-sample systems
5) Multimodal systems
6) Hybrid systems

B. Finding the Palm Print Traits by Its Finer Points

The main difficulty is how we convert the captured image into the template or in data streams. This difficulty is solved

by studying digital image processing. According to the theory-

1) X= Pixel value in Horizontal direction
2) Y= Pixel value in Vertical direction

This task can be accomplished by Pixelstick software available in the online market. In biometric characteristic, we take the physical or behavioral characteristic for identification (10, 1).

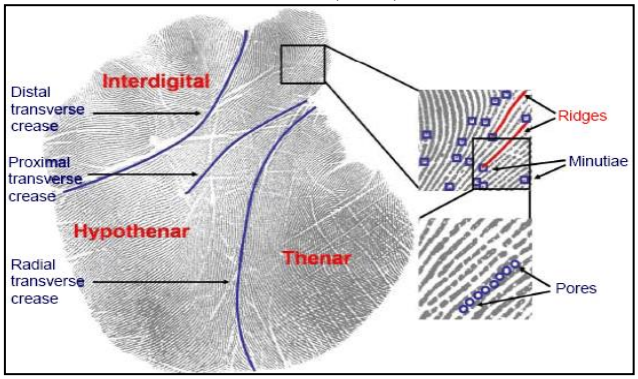

Fig. 8: Regions in Palm Print

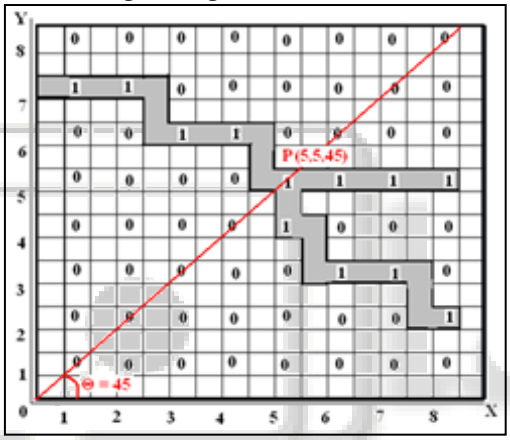

Fig. 9: Recognition of Palm Print Bifurcation

The systems are wide enforced for his or her easy use, public acceptance, and integration capabilities. One amongst the shortcomings of the hand pure mathematics characteristic is that it's not extremely distinctive, limiting the applications of the hand pure mathematics system to verification tasks solely.

1) 36 Feature Extracted from Palm Print Image

- Finger length (FL) x 4
- Finger sub-length (SL) x 12
- Finger width (FW) x 8
- Palm length (PL) x 1
- Palm width (PW) x 1
- Hand length (HL) x 1
- Hand contour length (HCL) x 1
- Hand area (HA) x1
- Fingertip location (FTL) x 4
- Gap between fingers location (GFL) x 3

2) 36 Feature Extracted from Face Image

- Red Spots (RS) x 14
- Green Spots (GS) x 11
- Distance (D) x 11

Fig. 10 (a): Applied Palm Print Impression

3) Applied Face Image of Clint

In order to obtain the similarity of the templates of both the Palm print image and the facial image, I have decided to take total of 36 finer points from both the images. For this purpose I have to use Pixel stick software to get X & Y fields of the images. Table 1 and 2 show that the templates of both the images. In this example 288 bits are required for storing X Field and Y Field. It means 576 bits are required to store a single template of either Palm print image or the facial image. Therefore the total bits required is-

576 + 576 = 1152 bits

In Multi-sample systems, the main advantage is the higher level of security. So that to compress the size of the chip I am combining both the templates of Palm print image or the facial image

S. No.	Bits for X - field		Bits for Y– field		Bits for C– field	
1	60	111100	71	1000111	131	10000011
2	62	111110	73	1001001	135	10000111
3	64	1000000	75	1001011	139	10001011
4	66	1000010	77	1001101	143	10001111
5	68	1000100	79	1001111	147	10010011
6	70	1000110	81	1010001	151	10010111
7	72	1001000	83	1010011	155	10011011
8	74	1001010	85	1010101	159	10011111
9	76	1001100	87	1010111	163	10100011
10	78	1001110	89	1011001	167	10100111
11	80	1010000	91	1011011	171	10101011
12	82	1010010	93	1011101	175	10101111
13	84	1010100	95	1011111	179	10110011
14	86	1010110	97	1100001	183	10110111
15	88	1011000	99	1100011	187	10111011
16	90	1011010	101	1100101	191	10111111
17	92	1011100	103	1100111	195	11000011
18	94	1011110	105	1101001	199	11000111
19	96	1100000	107	1101011	203	11001011
20	98	1100010	109	1101101	207	11001111
21	100	1100100	111	1101111	211	11010011
22	102	1100110	113	1110001	215	11010111
23	104	1101000	115	1110011	219	11011011
24	106	1101010	117	1110101	223	11011111
25	108	1101100	119	1110111	227	11100011
26	110	1101110	121	1111001	231	11100111
27	112	1110000	123	1111011	235	11101011
28	114	1110010	125	1111101	239	11101111
29	116	1110100	127	1111111	243	11110011
30	118	1110110	129	10000001	247	11110111
31	120	1111000	131	10000011	251	11111011
32	122	1111010	133	10000101	255	11111111
33	124	1111100	135	10000111	259	100000011
34	126	1111110	137	10001001	263	100000111
35	128	10000000	139	10001011	267	100001011
36	130	10000010	141	10001101	271	100001111
TOTAL BITS		288+288=576				324

Table 1: For Palm Print Recognition System

S. No.	Bits for X - field		Bits for Y– field		Bits for C– field	
1	20	10100	21	10101	41	101001
2	22	10110	23	10111	45	101101
3	24	11000	25	11001	49	110001
4	26	11010	27	11011	53	110101
5	28	11100	29	11101	57	111001
6	30	11110	31	11111	61	111101
7	32	100000	33	100001	65	1000001
8	34	100010	35	100011	69	1000101
9	36	100100	37	100101	73	1001001
10	38	100110	39	100111	77	1001101
11	40	101000	41	101001	81	1010001
12	42	101010	43	101011	85	1010101
13	44	101100	45	101101	89	1011001
14	46	101110	47	101111	93	1011101
15	48	110000	49	110001	97	1100001
16	50	110010	51	110011	101	1100101
17	52	110100	53	110101	105	1101001
18	54	110110	55	110111	109	1101101
19	56	111000	57	111001	113	1110001
20	58	111010	59	111011	117	1110101
21	60	111100	61	111101	121	1111001
22	62	111110	63	111111	125	1111101
23	64	1000000	65	1000001	129	10000001
24	66	1000010	67	1000011	133	10000101
25	68	1000100	69	1000101	137	10001001
26	70	1000110	71	1000111	141	10001101
27	72	1001000	73	1001001	145	10010001
28	74	1001010	75	1001011	149	10010101
29	76	1001100	77	1001101	153	10011001
30	78	1001110	79	1001111	157	10011101
31	80	1010000	81	1010001	161	10100001
32	82	1010010	83	1010011	165	10100101
33	84	1010100	85	1010101	169	10101001
34	86	1010110	87	1010111	173	10101101
35	88	1011000	89	1011001	177	10110001
36	90	1011010	91	1011011	181	10110101
TOTAL BITS		288+288=576				324

Table 2: For Facial Recognition System

By combining the data of X Field and Y Field it is observed that only 324 bits will be required for storing each the templates of both the images. Therefore the total bits required is-

$$324 + 324 = 648 \text{ bits}$$

$$\text{This gives the Compression Ratio} = \frac{1152-648}{1152} \times 100\%$$

$$\text{Compression Ratio} = \frac{504}{1152} \times 100\% = 44\%$$

VI. Conclusion & Future Works

All human faces share an analogous topological structure. Wiskott et al. gift a general in-class recognition technique for categoryifying members of a famed class of objects. Faces square measure delineated as graphs, with nodes positioned at fiducial points (such because the eyes, the tip of the nose, some contour Points, etc.) and edges tagged with 2-D distance vectors. Finally, so as to complement the face description, any fiducial points (red points in Figure 7) square measure inferred on the premise of the position of the extracted points. In future the Palm print and also the fingerprint pictures are going to be united to urge the radical high level of security. I actually have given the concept of enhancing the protection in Multi-sample systems with achieving the compression that is that the most important parameter for biometric systems. In future, I shall use an efficient committal to writing technique to urge this trend to the best level of security.

References

[1] G. Kaur S. Bhushan and D. Singh, "Fusion in multimodal Biometric Systems: A Review", Indian Journal of Science and Technology, pp. 1 – 10, July 2017.
[2] Madhavi Gudavalli, Dr. S. Vishwanadha Raju, Dr. A. Vinaya Babu and Dr. D. Srinivasa Kumar, "Multimodal Biometric– Sources, Architecture & Fusion Techniques: an overview", International Symposium on Biometric and Security Technologies, pp. 1 – 10, 2012.
[3] Wayman J, Jain A, Maltoni D, Maio D., "An introduction to biometric authentication systems", Biometric Systems 2005; 1–20.
[4] Ross A, Jain A. K., "Multimodal biometrics: An overview", 12th European Signal Processing Conference, 2004 Sep 6, pp. 1221–4. PMid: 14982620.
[5] Ross A, Jain A. K., "Information fusion in biometrics", Pattern recognition letters", 2003 Sep 30; 24(13):2115–25.
[6] Prathipa C and 2Latha L., "A survey of biometric fusion and tem¬plate security techniques", International Journal of Advanced Research in Computer Engineering and Technology. 2014; 3(10):3511–6.
[7] Ghayoumi M. A., "review of multimodal biometric systems: Fusion methods and their applications", IEEE/ACIS 14th International Conference on Computer and Information Science (ICIS), 2015 Jun 28. pp. 131–6.
[8] Jain A., Nandakumar K, Ross A., "Score normalization in multimodal biometric systems", Pattern recognition. 2005 Dec 31; 38(12): 2270–85.
[9] Jaafar H., Ramli D. A., 'A review of multi-biometric system with fusion strategies and weighting factor", International Journal of Computer Science Engineering (IJCSE). 2013; 2(4):158–65.
[10] K. Jain, A. Ross and S. Prabhakar, "An introduction to biometric recognition". IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, pp. 4–20, Jan 2004.
[11] Chander Kant, Rajender Nath, "Reducing Process-Time for Fingerprint Identification System", International Journals of Biometric and Bioinformatics, Vol. 3, Issue 1, pp.1- 9, 2009.

