ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

# An Encryption Technique using Fusion of Multi-Biometrics Data and Prim Numbers

Mr. Kadtan Mahesh Narayan[1], Dr. Mrs. Sadhana Chidrawar[2]

M.E. Student, Department of Computer Science Engineering, MPGI SOE College, Nanded, Maharashtra, India[1]

Dean, Department of Computer Science Engineering, MPGI SOE College, Nanded, Maharashtra, India[2]

**ABSTRACT**: Since from last decade, there is significant attention paid by research communities on the Join Directors Laboratories (JDL) to solve the conceptual and structural problems related to the multi-sensor data fusion. We exploited the JDL concept by fusing the heterogeneous data such as multi-biometric and RSA keys for the efficient user authentication and access control in many real time applications. We used the two biometrics such as face and fingerprint biometrics to combine with the public key cryptography using the information fusion (IF) methods. The proposed method not only delivers the person identification but also perform the biometric data encryption. The novel algorithm proposed in this project to do the fusion of face biometrics, fingerprint biometrics and numerical data. This algorithm is based on hybrid information fusion called the FFIF (Face-Fingerprint Information Fusion). We use the digital face and fingerprint as biometric component and two prime numbers as the numerical components based on RSA algorithm.

**KEYWORDS:** Biometric sensor, multi-biometrics, cryptography multi-biometric fusion.

## I. INTRODUCTION

The act of utilizing more than one biometric methodology, test, sensor, or calculation to accomplish acknowledgment, ordinarily alluded to as multi-biometrics, is a system that is quickly picking up notoriety. By joining multi-biometrics into the acknowledgment procedure, a large number of the weaknesses of conventional single-biometric frameworks can be reduced also, by and large, acknowledgment exactness can be improved.

Multi-biometrics can intrinsically build framework vigour by expelling the reliance on one specific biometric approach. Further, a framework that uses more than one biometrics highlight or matcher might be increasingly hard to intentionally parody. Frameworks that make utilization of various biometric highlights can likewise give repetition that may bring down the inability to obtain rates. While examination into multi-biometrics has gotten a vast increment in participation over ongoing years, the assignment of combining numerous biometric modalities from a solitary sensor remains an under-considered test. Because of an absence of accessible multimodal information, numerous present tests in multi-biometrics make "illusory" datasets, in which tests of one biometric methodology from one lot of subjects are discretionarily combined with a second biometric methodology from a different arrangement of subjects so as to mimic a multi-biometric situation. Biometrics are found in various fields [1], including therapeutic applications, for example, body measurements and blood classification, regular science ponders, for example, changes in the development of the human species, and sociologies, for example, changes in the humanities of the human species, however, is presumably most generally known for its utilization in criminal legal sciences and data security administrations extending from validation to key inference. Today the utilization of biometrics in security, applications are an integral part of our regular daily existences. The spread of biometrics was activated by two elements: specialized progressions and a requirement for security. The requirement for exceptional sensors to acquire biometrics was for quite some time considered a burden, particularly if multi-biometrics was considered. Today dependable biometric information can be acquired all the more effectively with ordinary gadgets being interconnected and having the capacity to assemble sensor information [2], [3], with advances in sensor equipment [4], [5]. For instance, a cell phone has a huge number of potential biometric sensors, some for this very reason, like a unique finger impression scanner, and others that can

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

catch biometrics as an optional capacity, for example, a high-goals camera, for face acknowledgment, iris and retina filters, a mouthpiece for voice recording, and inertial sensors for step. Obviously, these equivalent gadgets could likewise be abused to assemble individual information, requiring further thought about framework security [6], [7]. Security concerns are the second factor for the reception of multi-biometrics. In spite of the fact that there are numerous worthy ways to confirm individuals biometrics give the most grounded proof that the individual being referred to is really included, for example, a secret key could be given to another person. Generally nations have executed eIDs, which incorporate biometric components on travel papers and IDs, however, some have additionally made an interesting computerized The ID for the subject as a computerized endorsement/private key, for example, venture Stork [8], for imperative online exchanges like duty filings. Biometrics likewise offers a few extra security favourable circumstances, for example, great entropy when used to infer encryption keys, non-denial, and negative acknowledgment. A negative acknowledgment is helpful in situations where a client ought to be kept from denying being as of now taken a crack at the biometric framework, consequently recognizing endeavours at twofold enlistment utilizing a false name.

Aim of this research work is to design the security and person identification algorithm based on information fusion techniques. The objectives are:

- To present the study on various security solutions based on biometrics and public key cryptography.
- To study the importance of person identification and authentication

## II. LITERATURE SURVEY

The concise history of innovative work of information recovery framework beginning with the making of electro-mechanical looking devices, through to the early appropriation of PC scan for things that are pertinent to client's solicitation is portrayed in [34]. It additionally portrays the advances accomplished by Information Recovery inquires about from the 1950s through to the present day, concentrating on the way toward finding significant information. directing a few special cases that the utilization extent of data on the face recognition issue has been set up as observing three dimensional (3D) things from two-dimensional (2D) pictures. Previous strategies viewed this as a 2D recognition issue. Face recognition first endeavored during the 1960s (Bledsoe, 1964) and 1970s (Kelly, 1970). Amid the mid-1990s, testing toward FRT has developed essentially. One can accept recognition this to a few reasons: one is a fervor toward trade openings and openings; second is the receptiveness of frameworks, and the developing of observation elated application over the range of late years. Investigation has concentrated on the most ideal approach to make face recognition frameworks completely adjusted by dealing with issues, for instance, obstacle of a face in a given picture or highlight cut and extraction of unconventionality, for instance, eyes, mouth, and so forth., In the meantime, huge imaginative advances have been made in the setup of classifiers for beneficial face recognition. Among appearance-based broad procedures, eigenfaces[9]. In [10] they have wound up being persuading in examinations with vast databases. Highlight based picture looking at frameworks in[28] have been actually amazing and showed up distinctively in association with a broadly comprehensive approach, typically based frameworks are less touchy to groupings in the enlightenment and perspective and to bungle in neighbor go up against. In any case, the component extraction strategies required for this kind of approach are as yet not strong or adequately right Since the last five to eight years, a wide investigation has been engaged around video-based face recognition. For instance, drivers' licenses, because of the controlled method for the photograph securing framework, the division issue is conspicuously direct. If a part game-plan is open, the division of a moving person could be all more effectively wrapped up by using advancement as a sign. Meanwhile, the little size and low picture nature of appearances got from highlights can essentially inconvenience the recognition framework. In AI authentic learning is additionally related, for the event, incorporating condition have a fundamental impact in observing faces in association with a display.

Encryption can be characterized as the change of the data into a type of another structure where that can't be comprehended by numerous individuals without decoding the encrypted data. Decoding is the turnaround procedure of encryption. In this area, we are talking about a portion of the current data encryption procedures. In[11] proposed an encryption strategy with upgraded Various Huffman Table (MHT) by key bouncing technique. The recently built up Various Huffman Table (MHT) has great attractive properties yet it was very helpless against the picked plaintext assault (CPA) Though this improved MHT encryption technique faces every single such impediment. As the outcome appeared,

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

that the calculation is secure for the picked plaintext assault and demonstrated numerically by the key jumping method[12]. In [13] exhibited an original copy for Ordering the Encryption Calculations as per the Example Recognition technique. In this article, the writers center around the constraints of the calculations which are utilized for encryption plot and for creating the keys for the encryption procedure. Here the example recognition strategy to recognize the square figures in the encryption process. The square figure calculations like AES, DES, Thought, and RC were utilized to recognize the great arrangement method. As the outcome appeared, that the execution of RoFo (Revolution Timberland) classifier has great grouping exactness.

In[14] creator joined face, fingerprint and hand geometry at the coordinating score level. In[15]presented multimodal individual confirmation framework utilizing hand pictures by consolidating hand geometry and palm picture at the element level and match score level. The combination at the match score level had great execution when contrasted with unimodal biometric. In[16] the creator built up a multimodal biometric framework utilizing hand geometry, fingerprint, and voice at match score-level combination. In[[17] creator utilized hand veins, hand geometry, and fingerprint to give high security. In[18] joined iris and fingerprint to improve the execution. In[19] coordinated palm print and fingerprint at the element level. In[7] exhibited multimodal finger veins recognition utilizing score level melding for finger geometry and finger veins. In[14] exhibited palm and face multimodal biometrics for little example estimate issues. They utilized a Gabor channel to separate highlights of palm and face pictures. In[15] introduced multimodal iris and discourse validation framework utilizing choice hypothesis

## III. PROPOSED APPROACH FRAMEWORK AND DESIGN

***Biometric and Numerical Information Fusion***

Biometric and Numerical Information Fusion (BNIF) calculation is to join the finger code and numerical fragment to make an access key for the secured trade of electronic money related benchmarks. In the going with, showing a once-over of the key times of the system which makes the mix of information possible

The arrangement is disengaged into three areas:

1. Fingerprint Calculation: it is for isolating the biometric code;
2. RSA: it is for making the number code and the private key;
3. It is for information mix articulations

Fig 1: shows the structure plan, here use two sources fingerprint and bit information. In any case, input the fingerprint and changed over into a novel imprint fingerprint code [1]. Through the component extraction calculation, separate the biometric features of the biometric fingerprint, which is used for the half breed fusion vector. By then, you can get the columnist of fingerprint code, as a numerical vector. Around at that point, input a touch of information and taking care of by a safe RSA calculation to get the private key vector and a module vector. The module vector incorporates the result of two prime numbers. By then, solidify the interesting fingerprint code and private key and module vector from bit information to shape the mixture face code by Biometric and Numerical Information Fusion (BNIF) calculation [1]. The half breed fusion vector utilized as a character of the genuine user. BNIF utilized for the change of two vectors into one system that is mix fingerprint code, module, and private key vectors.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

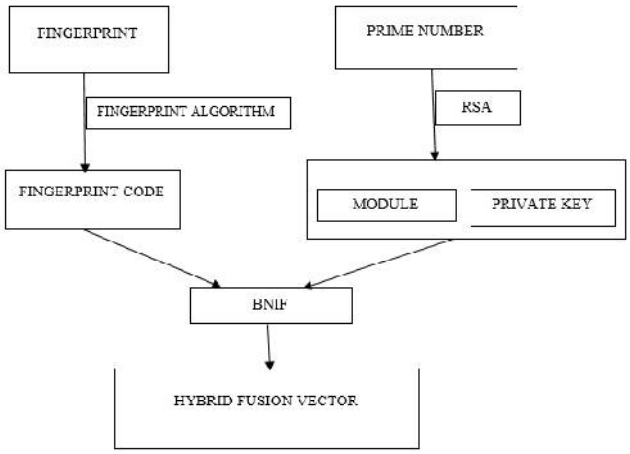


Fig 1: System Architecture Using BNIF Algorithm

In BNIF calculation, fingerprint code, module and private key as the numerical vectors with different sizes. Crossbreed Fusion vector is formed by cushioning the fingerprint, module and private key vectors by BNIF calculation. For cushioning activity, need to try and out the range of the vectors.

The change two vectors into one vector by BNIF Calculation step is given underneath:

- Be a and b € Z, a and b are two vectors, where a contains the biometric component and b the product of two prime numbers.
- Be s € Z: s = m +n; a whole number containing s root.
- In order to have a square root, it is necessary that
- nz1= q-mod (m .q) and nz1= q-mod (m .q).
- So the new dimensions of the vectors will be:
- m1 = m+nz1 and n1 =n+nz1.
- In addition, divide each vector into blocks which will be the lines of the hybrid vector, a vector containing the two vectors inserted in a proper way,
- nbloocc_a1 = m1/q and nbloocc_a1 = n1/q.
- Be: Pad = nz1 + nz2,
- In order to insert the blocks is given by the private key; value of the first component of the private key defines the no of the blocks of the face code vector to be inserted into the hybrid vector and the second component of the private key define the no of blocks of the module vector to be inserted into the hybrid vector and so on.
- Finally, the algorithm has to verify that the obtained matrix is really squared as,
- PadTot = q2 − (m + n),
- Diff = P ad – PadTot
- Then, three cases can be distinguished:
- Diff < 0 =⇒ addition of a line,
- Diff = 0 =⇒ no added padding,
- Diff > 0 =⇒ addition of a column.
- The padding line or column to be added id created using the private key.
- When you fabricate the squared Union U matrix, a post-result of grid U and permutation matrix P is done, henceforth you get a difference in sections. The private key of the cryptography of the calculation picks the

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

permutation matrix. This framework, whose measurements are like the ones of matrix U, is formed consolidating six 3×3 frameworks of change, got from a similar grid:

- At long last, you include the result of Union Matrix U and permutation P framework:
- F= UP
- Fusion F framework you acquire will be separated and organized along the lines to fabricate the yield V vector that is the Hybrid Finger Code.

**B) Face Information Fusion:**

The FIF Calculation is to join the face picture of the client and a bit data to shape an exceptionally remarkable vector [3]. In the going with, you can see the piece plot showing a summary of the chief times of the system, which makes the information blend.

The arrangement is apportioned into three areas:

I. Face Calculation: it is the fragment for isolating the biometric code;

II. RSA: it is the fragment for making the number code and the private key;

III. FIF Calculation: it is the part for the information blend

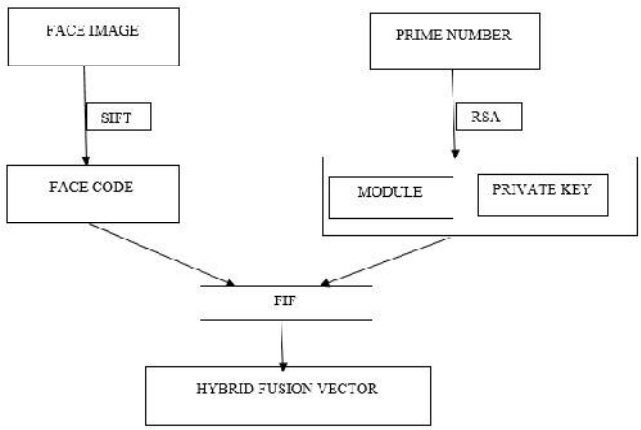


Fig 2: System Architecture Using FIF Algorithm

Fig 2: exhibits the structure, here use two information sources face the picture of the genuine client and bit information. To begin with, transfer the picture of the certifiable customer, and changed over into a face code. Through the Filter, calculation separates the biometric features of the image which is used for the crossbreed face code. A filter is a calculation in PC vision to recognize and depict nearby highlights in a picture. By then, you can get the columnist of a face code, as a numerical vector. Around then, input a touch of information and getting ready by secure RSA calculation to get the private key vector and a module vector. By then, unite the face code and private key and module vector from bit information to outline the crossbreed fusion vector by Face Information Fusion (FIF) calculation. FIF calculation utilized for the change of two vectors into one lattice that blends face code, module, and private key vectors. The half breed fusion vector can in like way go about as a passageway key.

The calculation of Face Information Fusion goes for getting a Fusion Key start from biometric and numerical data. A critical time of this calculation is the difference in two vectors into one vector. It is fundamental that this network is squared and that its solicitation depends upon the amount of the portions of the two vectors.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

The FIF calculation steps are given beneath:

- Be a, b € Z, two vectors, where a contains the biometric component and b the product of two prime numbers.
- Be s € Z :
- s=m + n; where m and n are the sizes of the biometric vector and module vector.
- Be q € Z :
- q= [√ s] a whole number containing s root.
- To reduce the size of two vectors by,
- nz1 = q-mod (m. q) and nz2 = q-mod (n. q).
- The new size of the vectors is given by,
- m1 = m+nz1 and n1 =n+nz1.
- In addition, divide each vector into blocks which will be the lines of the hybrid vector, a vector containing the two vectors inserted in a proper way,
- nbloocc_a1 = m1/q and nbloocc_a1 = n1/q.
- Be: P ad = nz1 + nz2,
- In order to insert the blocks is given by the private key; value of the first component of the private key defines the no of the blocks of the face code vector to be inserted into the hybrid vector and the second component of the private key define the no of blocks of the module vector to be inserted into the hybrid vector and so on.
- Finally, the algorithm has to verify that the obtained matrix is really squared as,
  PadTot = q2 − (m + n),
  Diff = P ad – PadTot
  Then, three cases can be distinguished:
  Diff < 0 =⇒ addition of a line,
  Diff = 0 =⇒ no added padding,
  Diff > 0 =⇒ addition of a column.
  The padding line or column to be added id created using the private key.
- When you fabricate the squared Union U matrix, a post-result of grid U and permutation matrix P is done, henceforth you get a difference in sections. The private key of the cryptography of the calculation picks the permutation matrix. This framework, whose measurements are like the ones of matrix U, is formed consolidating six 3×3 frameworks of change, got from a similar grid:
- At long last, you include the result of Union Matrix U and permutation P framework:
- F= UP
- Fusion F framework

## IV. RESULT

The experimental results of the proposed approach have been presented in this section. The proposed approach is implemented in Matlab. We have tested the proposed approach with different sets of fingerprint and Face. First we take the input fingerprint image, the extracted minutiae points.

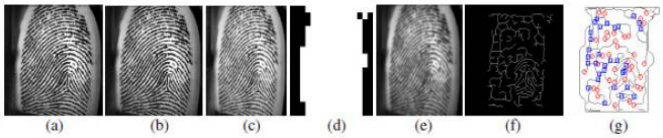


Figure 4.3 (a) Input fingerprint image (b) Histogram Equalized Image (c) Wiener Filtered Image (d) Segmented Image (e) Enhanced image (f) Morphological Processed Image (g) Fingerprint image with Minutiae points.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

Then you can get the correspondent of a face code Figure 4.4 as a numerical vector:

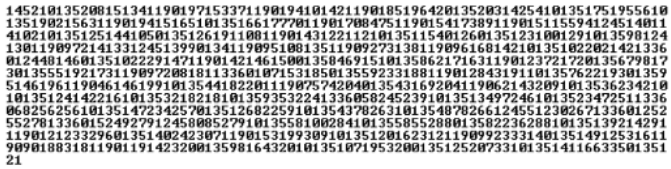

Figure 4.4 Face Code

The product of the two prime numbers (module) 4.5 and the private key (1024 bit) 4.6 are obtained with RSA algorithm

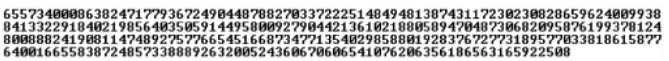

Fig. 4.5. Product of 2 prime numbers (Module)

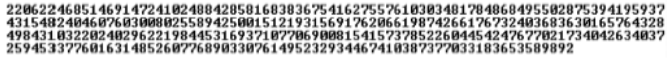

Fig. 4.6. Private Key

By the fusion of these data, as we have explained before, we get Hybrid Code figure 4.7 containing previous information arranged in an order which seems quite random to an intruder's eyes.

Fig. 4.7 Hybrid Code

## V. CONCLUSION AND FUTURE WORK

We present the Hybrid Information Fusion algorithm, called FFIF. We have attempted to generate a secure cryptographic key by integrating multiple biometrics modalities of human being, so as to provide better security. An efficient approach for generation of secure cryptographic key based on multimodal biometrics (Face and fingerprint) has been presented in this paper. In this methodology fingerprint traits have been integrated in the RSA algorithm and face biometrics to develop a new asymmetric cipher system. We select fingerprint to improve efficiency because it offers accurate identification method also fingerprint are mostly accepted biometrics among the technology. A possible application of this technique of encryption is associated with the authentication of a person, for example, to guarantee the security of electronic currency transactions such as the access to very private areas, to classified and confidential documents, privileges to activate critic, military or defensive infrastructures, etc.

Future works are aimed extend the proposed approach to several distinctive biometric traits. Quality metrics and partial-face matching will be introduced, and run-time analysis will be conducted.

## REFERENCES

[1]. Gerardo Iovane and Michele Nappi," An Encryption Approach Using Information Fusion Techniques Involving Prime Numbers and Face Biometrics", 2018.

[2]. G. Iovane, A. Amorosia, E. Benedetto G. Lamponi, "An Information Fusion approach based on prime numbers coming from RSA

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

*(A High Impact Factor, Monthly, Peer Reviewed Journal)*

*Visit: www.ijirset.com*

**Vol. 8, Issue 5, May 2019**

algorithm and Fractals for secure coding", 2015
[3]. B.V. Dasarathy, "Information fusion - what, where, why, when, and how?" Information Fusion, 2(2):75–76, 2001.
[4]. E. Waltz and J Llinas, ".Multisensor Data Fusion"., Artech House, Inc., 1990.
[5]. K. I. Chang, K. W. Bowyer, S. Sarkar, and B. Victor, "Comparison and combination of ear and face images in appearance-based biometrics", pp. 1160–1165, 2003.
[6]. M.Manzo E.Sangineto L.Cinque, G.Iovane. Face recognition using sift features and a region-based ranking. *Journal of Discret Mathematical Sciences and Cryptography*, 13(2):153170, 2010.
[7]. Department of Defence. Data fusion subpanel of the joint directors of laboratories, technical panel for c3. data fusion lexicon, 1991.
[8]. Department of Defence. Dsto (defence science and technology organization) data fusion special interest group. data fusion lexicon, 1994.
[9]. E. Waltz and J Llinas, ".Multisensor Data Fusion"., Artech House, Inc., 1990.
[10]. Chen, S., Jain, A.K., 1998. A ®ngerprint matching algorithm using dynamic programming. Technical report, Department of Computer Science and Engineering, Michigan State University.
[11]. Fabian Dreher, Tony Samuel "Continuous images of Cantor's ternary set" arXiv: 1303.3810.
[12]. Clinton P. Curry "Irreducible Julia sets of rational functions" Journal of Difference Equations and Applications, Volume 16, Issue 5 & 6 May 2010, pages 443-450.
[13]. G.Iovane, L.Puccio, G.Lamponi, A.Amorosia. Electronic access key based on the innovative Information Fusion technique involving prime numbers and biometric data. Journal of discrete mathematical sciences and cryptography. Taru Publication, 2010.
[14]. N. Ruggeri. Principles of pseudo-random number generation in cryptography, University of Chicago, 2006
[15]. Ross A (2007) An Introduction to Multibiometrics, Proceedings of the 15th European Signal Processing Conference (Poznam, Poland)
[16]. G. Mary Amirtha Sagayee, S Arumugam, and G.S.Anandha Mala(2013), Biometric Encryption using Enhanced Finger Print Image and Elliptic Curve,IJCSNS , VOL.13 No.7, July 2013:106- 113.
[17]. L. Hong, A. K. Jain and S. Pankanti, \Can multibiometrics improve performance?," in Proceedings AutoID'99, (Summit(NJ), USA), pp. 59{64, Oct 1999.
[18]. G. Feng, D. Hu K. Dong, and D. Zhang, "When faces are combined with palmprints: A novel biometric fusion strategy", pp. 332–341, 2004.
[19]. C. H. Chen and C. T. Chu, "Fusion of the face and iris features for multimodal biometrics", pp. 571–580, 2006.