INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 4, Issue 2)
Available online at: www.ijariit.com

Survey on encryption approaches using information fusion with biometrics

Kavya R
kavyar132@gmail.com
St. Joseph's College of Engineering and Technology, Palai, Kerala

ABSTRACT

This comprehensive survey, tried to mention two encryption approaches to make an access key which can be utilized inside the field of computer security, and which can ensure an abnormal state of mystery, as well as, with an abnormal state of sureness, give a personal identity through Information Fusion (IF) methods. In particular, two non-associated zones have been joined, Biometrics and Public-key Cryptography. This decision was taken with a specific end goal to traverse the limits these two methodologies have discovered uniquely. In this review analysis, two algorithms Face Information Fusion and Biometric and Numerical Information Fusion.

Keywords: *Encryption, Information Fusion, Biometrics, Public-key Cryptography.*

1. INTRODUCTION

In the basic frameworks of a nation and additionally in those of the Protection or in the chronicles of ordered and secret reports of Open or Private Organizations, it is important to ensure the entrance as it were through the authentication of the user. From this point of view, an access key was produced to ensure not only an abnormal state of mystery, yet additionally, with an abnormal state of conviction, give a personal identity, utilizing biometrics, what's more, public key cryptography in the meantime. The previous is the best innovation to authenticate a person, utilizing one of the diverse biometric parts accessible, though to date the last is the method, which ensures the most grounded response to cryptographic attacks. The critical purpose of this survey concerns the combination of that heterogeneous information.

Information Fusion (IF) is a moderately current research field: information originating from additional than one source is at last combined with a specific end goal to get a super-data, where the wealth of subtle elements and the exactness of information are bigger than those you can get on the off chance that you treat information independently. Information Fusion is tied in with consolidating, or melding, data from various sources keeping in mind the end goal to encourage understanding or give information that isn't obvious from singular sources. There is a requirement for data combination in numerous zones, going from mechanical autonomy, where information from different sensors must be melded, to administration data frameworks, where data from various business procedures and sources must be coordinated. As Hall and Llinas (2001b) call attention to, the idea of information or data combination is not really new. All things considered, "multisensory information combination is normally performed by creatures and people to evaluate all the more precisely the encompassing condition and to distinguish dangers, in this way enhancing their odds of survival".

In 2008 a convention for arranging security was proposed, in view of the combination of a secret key and face biometric to authenticate the user [4]. The biometric coordinate is finished by module following up on the workstation of the client, who is verified as a versatile specialist originating from a protected server. In this work, utilizing the standards on which classical Information Fusion techniques are based, look at two inventive algorithms, which utilize a procedure of information combination. This is concentrated to permit the combination of heterogeneous information, for example, the key of a cryptographic algorithm based on primality and a biometric part (i.e. digital fingerprints, face image), henceforth making a hybrid cryptographic key. Furthermore, go for making, for an outside client, the strategy for the formation of another key created by the fusion algorithm however much irregular as could be expected, yet making this influenced by the key in light of primality.

Here inspect two algorithms to make an access key utilizing Information Fusion methods including prime numbers and physiological biometrics. The first algorithm is BINF algorithm consolidate digital fingerprint and a prime no to get a hybrid fusion code. The

second one is FIF (Face Information Fusion), consolidate face image of the user and a prime number to get the hybrid fusion code. These two hybrid codes utilized as an access key.

2. BACKGROUND

The Information Fusion is still an emerging field of research. Information Fusion field is usually viewed as a multidisciplinary investigate field including distinctive research zones (i.e. Data Mining, Knowledge Discovery, Artificial Intelligence, etc.)[5], portrayed themselves by a multidisciplinary and by particular research groups [6]. As the beginning stage, utilize the system proposed in [1]. This strategy has been subjected to fitting expansions. The technique already proposed produces recognizable proof codes to high security for confirmation measures.

While this approach consolidates Biometric code (Finger Code) and a numerical code in view of primality (RSA), to make a key encryption, by combining a numerical part, in view of primality (RSA Module), and an irregular number created by the fractal recipes[2]. As in [1], the development technique for the new code (key) created by the algorithm of fusion, will rely upon the private key of the RSA Algorithm. Encryption Approach Using Information Fusion Techniques Involving Prime Numbers, what's more, Face Biometrics make an entrance key with exceptional attributes[2][3].

3. INFORMATION FUSION INVOLVING PHYSIOLOGICAL BIOMETRICS AND PRIME NUMBERS

In the extensive survey, look at two algorithms postulations are identified with the Information Fusion techniques. First, one is BNIF-Biometric and Numerical Information Fusion algorithm, which consolidate fingerprint and prime number to frame a hybrid fusion code. The second one is FIF, which consolidate face image code and a prime number to form a hybrid face code.

Here look at two algorithms named FIF and BNIF algorithms. Those depend on the Information Fusion techniques including physiological biometrics, for example, the face recognition and fingerprint. The primary algorithm utilizes fingerprint as the biometric segment and the FIF algorithm utilizes face image of the user.

3.1. BNIF- Biometric and Numerical Information Fusion

BNIF algorithm is to join the finger code and numerical segment to create an access key for the protected exchange of electronic monetary standards. In the accompanying, you can see the block scheme [Fig. 1] demonstrating a rundown of the principal periods of the framework which makes the combination of information conceivable.

The plan is isolated into three sections:

- Fingerprint Algorithm: it is for separating the biometric code;
- RSA: it is for making the number code and the private key;
- BNIF Algorithm: it is for information combination. expressions:

Fig 1: demonstrates the framework design, here utilize two sources fingerprint and bit information. In the first place, input the fingerprint and changed over into a unique mark fingerprint code [1]. Through the feature extraction algorithm, separate the biometric highlights of the biometric fingerprint, which is utilized for the hybrid fusion vector. At that point, you can get the journalist of fingerprint code, as a numerical vector. Around then, input a bit information and handling by secure RSA algorithm to get the private key vector and a module vector. The module vector includes the product of two prime numbers. At that point, consolidate the unique fingerprint code and private key and module vector from bit information to form the hybrid face code by Biometric and Numerical Information Fusion (BNIF) algorithm [1]. The hybrid fusion vector used as an identity of the legitimate user.BNIF used to for the transformation of two vectors into one framework that is blend fingerprint code, module, and private key vectors.

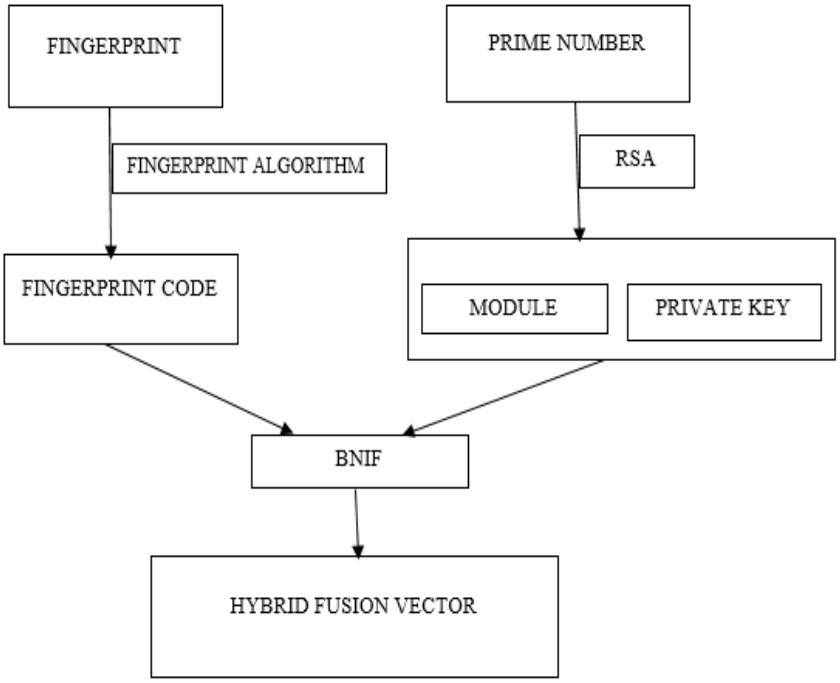

Fig 1: System Architecture Using BNIF Algorithm

In BNIF algorithm, fingerprint code, module and private key as the numerical vectors with various sizes. Hybrid Fusion vector is shaped by padding the fingerprint, module and private key vectors by BNIF algorithm. For padding operation, need to even out the span of the vectors.

The change two vectors into one vector by BNIF Algorithm 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 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.

3.2. FIF- Face Information Fusion

The FIF Algorithm is to join the face image of the user and a bit data to form a one of a kind unique vector [3]. In the accompanying, you can see the piece plot demonstrating a rundown of the principal periods of the framework, which makes the information combination.

The plan is partitioned into three sections:

- Face Algorithm: it is the segment for separating the biometric code;
- RSA: it is the segment for making the number code and the private key;
- FIF Algorithm: it is the part for the information combination.

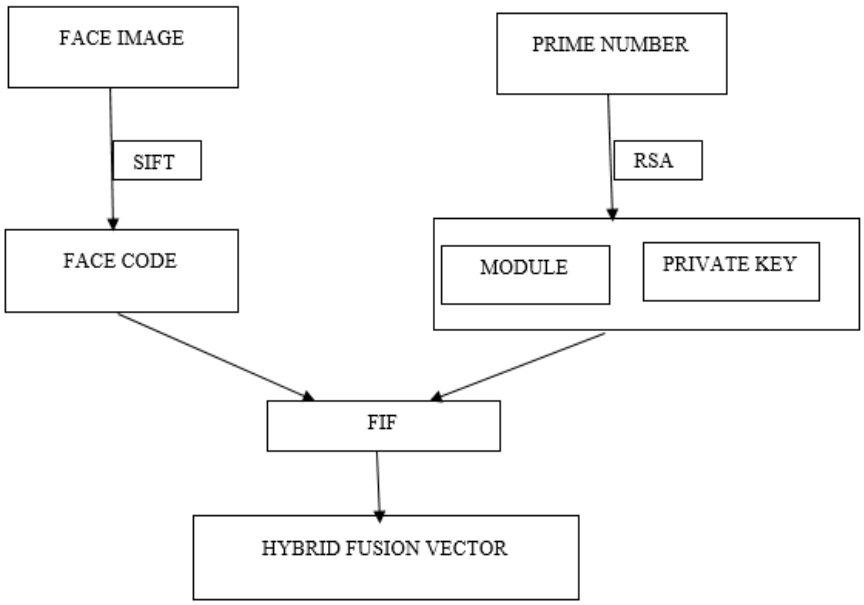

Fig 2: System Architecture Using FIF Algorithm

Fig 2: demonstrates the framework, here utilize two information sources face image of the real user and bit information. To start with, upload the image of the genuine client, and changed over into a face code. Through the SIFT algorithm separate the biometric highlights of the picture which is utilized for the hybrid face code. SIFT is an algorithm in computer vision to detect and describe local features in an image. At that point, you can get the journalist of a face code, as a numerical vector. At that, time, input a bit information and preparing by secure RSA algorithm to get the private key vector and a module vector. At that point, consolidate the face code and private key and module vector from bit information to frame the hybrid fusion vector by Face Information Fusion (FIF) algorithm. FIF algorithm used for the transformation of two vectors into one matrix that merges face code, module, and private key vectors. The hybrid fusion vector can in like manner go about as an entrance key.

The algorithm of Face Information Fusion goes for getting a Fusion Key beginning from biometric and numerical data. An urgent period of this algorithm is the change of two vectors into one vector. It is essential that this grid is squared and that its request relies upon the quantity of the segments of the two vectors.
The FIF algorithm steps is given below:

- 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 you acquire will be separated and organized along the lines to fabricate the yield V vector that is the Hybrid Face Code.

4. CONCLUSION

With the ascent in the security ruptures and extortion exercises, we require a system to demonstrate the authenticity of the client. The review endeavored to specify encryption algorithms utilizing information fusion techniques with physiological biometrics and a numerical part. The last yield the hybrid fusion code contains the unique characteristics of the user (Fingerprint code, Face code), which is utilized as a character of the legitimate user. By utilizing the hybrid fusion vector, to a degree can keep away from attacks like brute force attack, replay attack, and Phishing attacks, and can ensure that the user is legitimate or not. A possible application of this technique of data fusion is associated with the authentication of a person, for example, to guarantee the access to private areas, to classified and confidential documents, privileges to activate critic, military or defensive infrastructures, etc.

5. REFERENCES

[1] G. Iovane, L. Puccio, G. Lamponi, and A. Amorosia, “Electronic access key based on innovative Information Fusion technique involving prime numbers and biometric data”, 11 November 2014.
[2] G. Iovane, A. Amorosia, E. Benedetto G. Lamponi, “An Information Fusion approach based on prime numbers coming from RSA algorithm and Fractals for secure coding”, 2015.
[3] Gerardo Iovane and Michele Nappi,” An Encryption Approach Using Information Fusion Techniques Involving Prime Numbers and Face Biometrics”, 2018.
[4] G. Chetty, D. Sharma, and B. M. Balachandran, “An agent-based multifactor biometric security system”, Springer-Verlag, pp. 245–251, 2008.
[5] B.V. Dasarathy, “Information fusion - what, where, why, when, and how?” Information Fusion, 2(2):75–76, 2001.
[6] E. Waltz and J Llinas, “.Multisensor Data Fusion”., Artech House, Inc., 1990.
[7] 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.
[8] C. H. Chen and C. T. Chu, “Fusion of the face and iris features for multimodal biometrics”, pp. 571–580, 2006.
[9] G. Feng, D. Hu K. Dong, and D. Zhang, “When faces are combined with palmprints: A novel biometric fusion strategy”, pp. 332–341, 2004.
[10] L. Hong and A. Jain, “Integrating faces and fingerprints for personal identification”, IEEE transactions on pattern analysis and machine intelligence, pp. 1295–1307, 1997.

