*IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)*
*e-ISSN: 2278-2834,p- ISSN: 2278-8735.*
*PP 125-130*
*www.iosrjournals.org*

# Cryptographic Key Generation from Finger Vein;A Study

Sharon Davis[1] , Ayana John[2],Padmam Kaimal[3]
[1](Electronics and communication,Sahrdaya college of engineering and technology,KERALA,INDIA)
[2](Electronics and communication,Sahrdaya college of engineering and technology,KERALA,INDIA )
[3](Electronics and communication,Sahrdaya college of engineerinng and technology,KERALA,INDIA )

***ABSTRACT :***. *Biometrics in conjuction with cryptography forms a new progressive technology. Using biometric datas such as finger vein,face recognition,iris recognition and finger print for security purposes has become increasingly accepted.The use of biometric data in cryptography is a new, budding and capable area of research. One of the most important problems related with bio-cryptography is creation of a constant encryption key. This paper suggests the method of generation of cryptographic key from finger vein pattern. It is based on the established finger vein image pre-processing methods and a new algorithm.*

***Keywords*** *- information security,cryptographic key generation,biometrics*

## I. INTRODUCTION

The Information security plays an important role in protecting datas of a firm.But there are a lot of problems associated with the effectiveness of information security.Cryptography acts in an effective way to solve the problem of information security. In most of the cryptographic algorithms, cipher keys are used for encryption and decryption.But this causes some problems [4]. Simple users keys are not easy to be forget.But they can be cracked easily. But on moving to the case of complex keys,eventhough they are difficult to crack, they are difficult to remember.Also, the cipher keys may be illegally shared.So,all these problems should be solved.The biometric features which cannot be forgotten, stolen or cracked, is combined with the cryptography to form biometric cryptography. One of important problems facing in biometric cryptography is stable encryption key generation [4].Those keys must be generated truly, to contain sufficient entropy and be of enough length [1].One of the latest biometric methods is finger vein recognition [6,7]. The finger vein pattern based authentication method is highly reliable; veins are hidden underneath the skin surface so forgery is extremely difficult; it is non-invasive and easy to use, offering a balance of advantages. Finger vein patterns are unique for each and every human being. ERR in fingerprint based systems is much higher on comparing it with finger vein approaches. Thus,finger vein based authentication is very effective [8].Also,Riley et al. study [9] suggests that vein technology is more suitable compared to fingerprint technology. Fingerprint based technologies is very problematic because, fingerprints can be forged and the procedure of enrolment and scanning may be more difficult. In this paper the possibilities of key generation from finger vein patterns were explored

## II. LITERATURE WORK

The The initial technique involves stored pattern harmonizing to open a cipher key storage. If the user is authentic, the key is released. The next method hides the cipher key through a secret bit-replacement algorithm inside the enrolment pattern itself[9].Another method is to use data derived directly from a biometric image. In this method biometric data are used to generate a cryptographic key [10]. But one of the main drawback is that,the quality of biometric data depends on the person's physiological characteristics and also it is subjective by the environment.Thus, cryptographic key generation directly from biometric data is quite tough. There are many works, aiming to fill the gap between the fuzziness of biometrics and achieving cryptographic accuracy. This would enable keys to be generated directly from biometric images. The main problem is that biometric data is noisy and only an approximate comparison is possible with the template.

Topological fingerprint pattern minutiae point neighbourhood descriptors based approach has been proposed by Ushmaev et al. [11].The advantages are,these descriptors are very stable fingerprint features and don't depend on finger alignment and deformations. These approach allows varying decryption rates as well as key lengths. Stability of cryptographic keys is the core of bio-cryptography. Hu et al. [12] investigated the effect on the generated keys when an original fingerprint image is rotated. Investigation indicates that information integrity of the original fingerprint image can be significantly compromised by image rotation transformation process. It was revealed that the quantization and interpolation process can change the fingerprint features

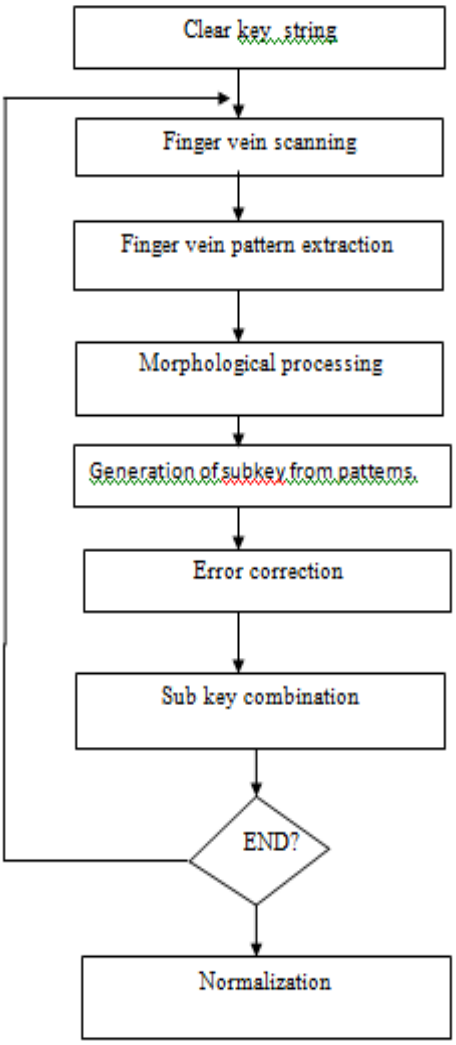
significantly without affecting the visual image.In Costanzo's [13] proposed method,it eliminates the need for template storage and shows how a cryptographic key can be made through the use of biometric feature. Zheng et al. [14] paper presents a lattice mapping based fuzzy commitment method for cryptographic key generation from biometric data. The method used ,outputs high entropy keys.Also it conceals the original biometric data such that it is impossible to recover the biometric data even when the stored information in the system is opened to an attacker. Wu et al [15] proposed a novel biometric cryptosystem.It is based on the most accurate biometric feature, iris.A textural feature vector is extracted from the pre-processed iris image by using a set of 2-D Gabor filters and a modified fuzzy vault algorithm is employed to encrypt and decrypt the data.. Previous works were mainly performed for generating keys using fingerprints. Here, proposed method deals with generation of cryptographic key from finger vein pattern.An infrared camera that captures the image that flows from a led array from the top of the device through the user's finger to the camera is used. The amount of light that will be delivered to the sensor will vary according to the user's finger thickness.To obtain high quality near-infrared (NIR) images, a special device was developed. Generally, finger-vein patterns can be imaged based on the principles of light reflection or light transmission [2].

## III. KEY GENERATION USING FINGER VEIN

In this paper a method for cryptographic key generation from finger vein pattern were demonstrated. A schematic representation for proposed method from finger vein patterns is shown in Fig.2.Through the method:Using multiple finger vein patterns, key is generated. Here, biometric method is combined with a password. The password is 'entered' by provide different finger sequences for the systems.Ten different finger vein patterns and combinations of enrolling these images to the system allows for virtually endless number of keys to be generated. Also longer keys and keys with higher entropy can be generated.First, vein pattern image is processed using conventional methods.Input to Contour Tracing Algorithm is the processed vein pattern and it is used to generate a partial cryptographic key. Partial cryptographic keys are concatenated to combine a final cryptographic key.A binary finger vein pattern FVP(a×b) is selected.It is further processed by Meaningful Coordinate Detection Algorithm (Fig. 2).MCD Algorithm is used to identify Region of Interest of blood vessel.For fixing ROI,(FIG.1)beginning point of vessel BP(a×2) and end point EP(a×2) and crossing vessel point coordinates CV(k×2) are considered. Finger vein pattern may be cropped depending on it's size so that we are able to make sure that to vein beginning and end points reach edges of the image.

Fig.1.Segmentation of ROI

Figure 1. Schematic representations of proposed cryptographic key generation method using finger vein patterns




Beginning and end points are found by scanning binary values along the edges of the image.Coordinates of intersections in the network are identified using a morphological branchpoints function.To allow and visualise user to select which BP, Meaningful coordinate Detection algorithm is used.To trace the contour Contour Tracing Algorithm is used (Fig. 3). The algorithm is used to identify which Vessel Beginning Points and which vessel end points are connected with a selected BP or EP. The contour is traced until a vessel intersection is detected. After an intersection is detected, all following branches are traced simultaneously. Fig. 4, shows a vascular pattern image with 100 initial contour points highlighted by Contour Trace Algorithm.

Figure 3.MCD Algorithm

Step 1:Initialize vessel beginning point matrix as BP;

Step 2: Initialize vessel end point matrix as EP;

Step 3 : Initialize vessel intersection point matrix; CP

Step 4: Initialize tracing point;

Step 5 :image should be resized (reduced) to required pixel level;

Step 6: Detection of BP from initial ;

Step 7:If the vein starting point is detected,then BP coordinates and assigned entrance numberas are noted;

Step 8: Detection of EP;

Step 9:If vein end point is detected ,then EP coordinates and assigned exit numbers are noted;

Step 10:End;

Figure 4. Contour Trace Algorithm

Step 1:Trace starting point

Step2:Trace directions through contour matrix.

Step3:Starting from tracing point,check all directions.

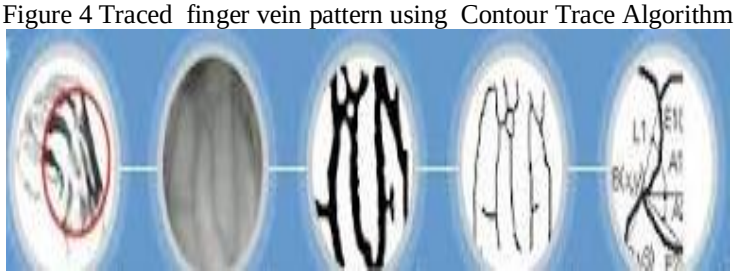
Step 4:If contour point detected,the record point coordinates

Step 5:Invert traced point value.

Step 6:End

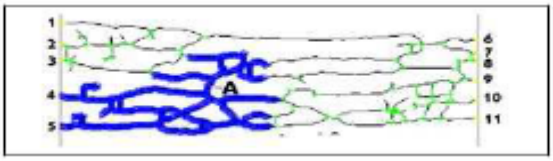
A binary finger vein pattern FVP(a×b) is selected.It is further processed by Meaningful Coordinate Detection Algorithm (Fig. 2).MCD Algorithm is used to identify Region of Interest of blood vessel.For fixing ROI,(FIG.2)beginning point of vessel BP(a×2) and end point EP(a×2) and crossing vessel point coordinates CV(k×2) are considered. Finger vein pattern may be cropped depending on it's size so that we are able to make sure that to vein beginning and end points reach edges of the image.

Figure 4 Traced finger vein pattern using Contour Trace Algorithm



A binary finger vein pattern FVP(a×b) is selected.It is further processed by Meaningful Coordinate Detection Algorithm (Fig. 2).MCD Algorithm is used to identify Region of Interest of blood vessel.For fixing ROI,(FIG.2)beginning point of vessel BP(a×2) and end point EP(a×2) and crossing vessel point coordinates CV(k×2) are considered. Finger vein pattern may be cropped depending on it's size so that we are able to make sure that to vein beginning and end points reach edges of the image.First tracing point is set as point number 4 and contour is traced. Figure 5 illustrates contour tracing at a point when first'exit' point (number 5) is reached after a fixed number of iterations of the Contour Trace Algorithm.After all BP and EP points are reached, the values assigned to each of these points are combined into one partial key in order of when they were hit by the Contour Trace Algorithm.

Figure 5. Contour Trace Iteration Method




## IV. ANALYSIS AND DISCUSSION

The contour is traced In Contour Trace Algorithm until a vessel intersection is detected. After it , all branches are traced simultaneously. An alternative operation is also possible.It is to trace one of the branches applying predetermined set of rules on how all following intersections should be crossed.The advantage of using Contour Trace Iteration Number Method is that, relatively small probability of error is obtained when the vein pattern image is altered insignificantly. The algorithm is robust.Because,it is affected by minor changes in the direction or position of certain veins in the pattern or any noise that is not directly connected to the main vein network.Managing additional loops, more complex junction structure and branches in the vein pattern is aso possible with this algorithm..This paper does not cover steps 4, 5 and 6 (Fig.1) of cryptographic key generation. Research of these key generation steps will be carried out in future work.

## V. CONCLUSIONS AND FUTURE WORKS

Generation of cryptographic keys from finger vein patterns is proposed in this paper.This method is used to generate a virtually limitless number of keys from finger vein characteristics of an individual. Without using any pre-captured samples or templates,Proposed Contour-tracing algorithm generates cryptographic key directly from finger vein patterns.In the future work all steps of proposed method of cryptographic key generation will be implemented and quality properties of the generated keys will be investigated. This algorithm is mostly misleading by incorrectly detected (or undetected) line connections in the main vein pattern and false BP/EP determination. Method generates incorrect code when vein pattern changes significantly shortens or lengthens certain sections of the vein images. Further research will be carried out to analyse Contour Trace Iteration Number Method properties and possibilities for improvement.

## REFERENCES

**Books:**

[1]. C. Tilborg (Ed). Encyclopedia of Cryptography and Security. Springer, 2005
[2]. Handbook of Information andCommunication Security, P. Stavroulakis,M. Stamp (Eds.), Springer, 2010

**Theses:**

[3]. U. Uludag, "Secure biometric systems,"Ph.D. dissertation, Michigan StateUniversity,http://biometrics.cse.msu.edu/Publications/Thesis/UmutUludag_SecureBSecureBio_PhD06.pdf, 2006.

**Proceedings Papers:**

[4]. Venckauskas, N. Jusas, I. Mikuckiene, S.Maciulevicius, "Generation of the secret encryption key using the signature of the embedded system", Information technology and control, T. 41, nr. 4, pp. 368–375, 2012.
[5]. Yao-Jen Chang, Wende Zhang, Tsuhan Chen, "Biometrics-based cryptographic key generation," Multimedia and Expo, 2004. ICME '04. 2004 IEEE International Conference on , vol.3, pp. 2203,2206 Vol.3, 27-30 June 2004.
[6]. J. Hashimoto, Finger "Vein Authentication Technology and Its Future", VLSI Circuits, Digest of Technical Papers. – pp. 5–8, 2006.
[7]. A. Venckauskas, N. Morkevicius, K. Kulikauskas, "Study of Finger Vein Authentication Algorithms for Physical Access Control", Electronics and Electrical Engineering, No. 5(121). – pp. 101–104, 2012.

[8]. N. Miura, A. Nagasaka ir T. Miyatake, "Automatic Feature Extraction from nonuniform Finger Vein Image and its Application to Personal Identification" IAPR Workshop on Machine Vision Applications, Dec. 11 - 13.2002, Nara- ken New Public Hall, Nara, Japan, 2002.
[9]. C. Riley, H. McCracken, K. Buckner,"Fingers, veins and the grey pound:accessibility of biometric technology",Proceedings of the 14th Europeanconference on Cognitive ergonomics(ECCE'07). – New York, [10]M. S. Al-Tarawneh,
[10]. L.C. Khor, W. L. Woo,and S. S. Dlay, "Crypto key generationusing contour graph algorithm", inProceedings of the 24th (IASTEDinternational conference on Signalprocessing, pattern recognition, andapplications (SPPRA'06), M. H. Hamza Ed.). ACTA
[11]. O. Ushmaev, V. Kuznetsov, V. Gudkov,"Extraction of Binary Features fromFingerprint Topology," Hand-BasedBiometrics (ICHB), 2011 InternationalConference on , vol., no., pp.1,6, 17-18 Nov.2011
[12]. Peng Zhang, Jiankun Hu, Cai Li,Mohammed Bennamoun, VijayakumarBhagavatula, "A pitfall in fingerprint biocryptographickey generation", Computers& Security, Volume 30, Issue 5, July 2011,pp. 311–319, 2011
[13]. C. R. Costanzo, "Active BiometricCryptography (ABC): Key GenerationUsing Feature and Parametric Aggregation,"Internet Monitoring and Protection, 2007.ICIMP 2007. Second InternationalConference on , vol., no., pp.28,28, 1-5 July2007
[14]. Gang Zheng, Wanqing Li, Ce Zhan,"Cryptographic Key Generation fromBiometric Data Using Lattice Mapping,"Pattern Recognition, 2006 2006. 18thInternational Confere. ICPR nce on , vol.4, pp.513–516, 2006
[15]. Xiangqian Wu, Ning Qi, Kuanquan Wang,Zhang D., "An Iris Cryptosystem forInformation Security", Intelligent Information Hiding and Multimedia Signal Processing, 2008. IIHMSP '08 International Conference on, pp. 1533–1536, 2008
[16]. J. Jagadeesan, T.Thillaikkarasi,K.Duraiswamy, "Cryptographic KeyGeneration from Multiple Biometric Modalities: Fusing Minutiae with IrisFeature", International Journal of Computer Applications 2(6), pp. 16–26, June 2010.
[17]. N. Miura, A. Nagasaka ir T. Miyatake,"Automatic Feature Extraction from nonuniformFinger Vein Image and itsApplication to Personal Identification"IAPR Workshop on Machine VisionApplications, Dec. 11 – 13.2002, Nara- kenNew Public Hall, Nara, Japan, 2002
[18]. N. Miura, A. Nagasaka ir T. Miyatake"Feature extraction of finger vein patternsbased on repeated line tracking and itsapplication to personal identification.