Finger Knuckle Print Authentication using Visual Threshold Cryptographic Techniques

Dr. A. Muthukumar
Department of Electronics and Communication Engineering
Kalasalingam Acadamy of Research and Education

Y. Tharun Babu
Department of Electronics and Communication Engineering
Kalasalingam Acadamy of Research and Education
Krishnankoil, India

K. Hemanth Kumar
Department of Electronics and Communication Engineering
Kalasalingam Acadamy of Research and Education
Krishnankoil, India

Y. Joshnakar Reddy
Department of Electronics and Communication Engineering
Kalasalingam Acadamy of Research and Education
Krishnankoil, India

***Abstract*—The proof uses signs, personal identification number. This will be easily goes into the hands of wrong persons. The tally will be unique with their identities. So the person can access to his information. Safety is the important theme of this project. Irrespective of the threat, everyone uses their identification as their protection, compared to identity Finger Knuckle Print will provide more secure and has their own separate stats. Sometimes, your stats will be theft. To overcome this, we use different typesof cryptographic techniques.This type of techniques have their own space to protect your data. To complete this Finger Knuckle Print algorithm, k - means algorithm,SIFTalgorithm and Shamir Secret Sharing can be used. Finger Knuckle Print has appropriate main points. These main points of Finger Knuckle Print was derived using different types of transforms. The secret hash value has protected data as the unknown or it is also called as the hidden value.**

Keywords—Visual threshold cryptography, finger knuckle print, Compression.

I. INTRODUCTION

The Biometric systems are being typically developed and deployed to boost security to users. biometric authentication or identification is employed to spot someone supported their structural or physiological characteristics like fingerprint, palm print, face, iris, footprint and finger knuckle print, etc. Finger knuckle print may be a new form of biometric systems that acknowledges someone supported the each knuckle lines and also the textures existing within the outer finger surface. These information's (line structures and finger textures) be ready to discriminate completely different people, as a result of it's comparatively stable and stay unchanged throughout the lifetime of someone. Finger knuckle print modality is far and away utilized by biometric systems owing to some blessings. First, information acquisition is comparatively easy and affordable via business low-resolution cameras. Second, Finger knuckle print based access systems are terribly adequate for indoor and out of doors usage, and may used even in extreme weather and illumination conditions. Third, Finger knuckle print options of adults aren't disposed to major changes they're a lot of stable over time. Finally, Finger knuckle print-based biometric data is incredibly reliable and it is with success used for recognizing individuals among many populations.

Principally finger knuckle print recognition divided into 2 tasks: (i) FKP identification and (ii) FKP verification. Before, the finger print examiners were put behind bars because of lack of challenges. These factors were need to be included: (i) The selected technique is the legit or it is a different type of mathematical derivations. (ii) The error rate was evaluated or not. (iii) Checking of long lasting techniques were existed and are maintained. (iv) Checking the complete noted review. (v) Checking whether it is general or unique type. The main core of common examine concludes the following: (i) The required amount of data is left out for the impression access before the differentiation. (ii) The amount of data is left out in accordance with a pair of impressions. The unique impression of one side is improved in different ways. This type of examine includes these factors: (i) The pair of impressions need to be same data to find out from different persons. (ii) It's hard to find a similar impressions from sample impression to find from different people, it can be verified using one side impression. If the sample and the impression are similar, then the person is authorized person. To protect from the false people. While pair of impressions are comparing with the different pair of impressions, it concludes the dimensions of finger also. We can notice that dimensions of one person are different with the other person dimensions. By checking the how much content of similarity is found from two or more impressions. From the concept, results of two or more other side examined. The finger impression can be authorized using offline mode or online mode. The offline mode can be done by using ink impression for the illiterate persons beside their name etc., The online mode can be done by using Finger print scanner it captures the snapshot of the impression for authentication. The online method is also called as live-scan method.

The offline method comprises of different types. They are rolled, dab, latent. In the rolled method, the ink is applied to the one side of the finger and impressed on the paper and rolled vigorously. Then, the paper is converted into grayscale image. The rolled fingerprints have a bigger ridge and furrow space because of the rolling method however have larger deformations because of the inherent nature of the rolling method. Dab is the completely different from the roll. In, dab the impression is not rolled. Latent is based on dimensions, and it's based on the sweat and oily in the surface of the finger. A live-scan fingerprint is confronted from the scanner despite of using the paper. The scanner has sensors that reads the data of the finger placed on the surface of the scanner. The sensors read different variety of data from the impression.

The live-scan sensors impression can be measured from the different types of techniques. The ultrasonic-based impression sensors have dimensions but we can't be used regularly. A biometric authorization are comprised of two types. 1) Authentication type. 2) Individuality type. From the authentication type, authorization when in operation its rejects or accepts the authentication of a person, where as in the individuality type, its operation mostly declines the authentication of a person. There are many limitations in this authentication.13 There are different types of applications in the authentication mode, daily attendance of an employee in office it notes the accurate time. This also has different types: (i) enrolment (ii) authentication The enrolment method enrolls the person data for future references, whereas the authentication method is to access the already enrolled person for repeated number of times. Enrolment is a difficult system compared to authentication.

II. RELATED WORKS

During the studies of multiple increased techniques in VC we have a tendency to found a noteworthy space to implement the prevailing ideas. Being awake to the sure problems regarding authentication management like spoofing Associate in Nursing "buddy punching" we have a tendency to are attempting to introduce Associate in Nursing application supported statistics. After concluding the impression image as the unknown image. The distribution of shares could be done. One share to the data storage system and the other share to the details extraction. This causes theft problems. It has only two shares. First share collects the data of the person and it stores the concerned person's data in the data server. The second share is with the concerned person which required for the access during the details matching check process. With only two shares present its unable to do the decryption process. By scanning the person's fingerprint, it checks the system share image with the person's share image during the details extraction. The process succeeds if the match is similar.

III. OUR CONTRIBUTION

But here we are supposed to use any of the one at a time to identify the user. So, authentication results are more secured. Now we are using password and smartcards to confirm the user who is approved for the card or to their belongings. However, passwords and cards easily hacked so that the users don't know about the details that were be cracked. In our paper we are going to implement new biometric symbol that is knuckle finger as shown in the first figure. We know several researches are going on based biometric,but using knuckle as biometric is new raising method to identify the user. This knuckle print identification system consists different process like acquisition,extraction, confiscation, MATLAB coding and matching. Here we are doing to analyze the back side of the finger that is known as knuckle finger and we are going to match it with fourier rework and physicist filter at several times.

The inner information of the knuckle finger was accessed with Scale Invariant Feature rework and Speed Up strong options . The scale invariant algorithmic program is used make the key words of the victim to prove the exact user. We also planned a new technique of triangulation. The fingerprint recognition was finished at the stage of image segmentation, K- means of that cluster. Orthogonal linear Discriminant analysis was done to acknowledge the Finger knuckle print at the side of Gabor filter with its key. In this process of making secure the or to identify the exact user cryptography plays a major role. However these keys are definitely cracked by the different persons who are not authorized. So we supposed to use the several keys but it is not possible to store in human memory. We can thank the biometric values that it will store more data and more number of keys can be stored for longer time makes it more confidential using some cryptography techniques it will makes more secure. We are using cryptography of different kinds like visual and threshold and also we are using combining both visual threshold cryptography technique.The major25 role of Biometric Cryptosystem is to give a lot of security and authentication compared to the other password and cards. Cryptography provides an associate algorithmic program to convert normal text into cipher in different format which can be known to only sender and receiver alone. cryptographical technique is mainly classified into two types first one is isosceles cipher in which typical secret codes where used for each cryptography method. Second one is uneven cipher in which public secrets used for cryptography method. Mostly we are going to use isosceles cipher.

Here we are going to use the SIFT rule. For inner option of a knuckle pictures.

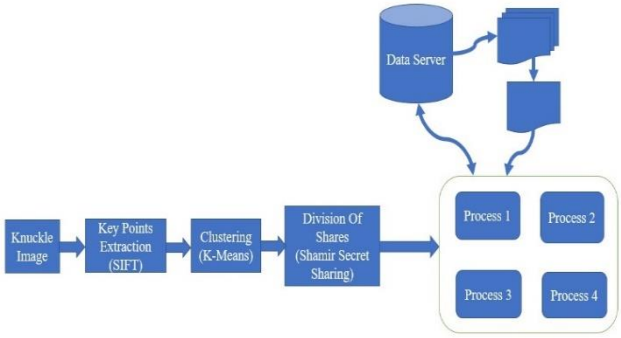


Fig.1Finger Knuckle Print Based Threshold Visual Cryptography authentication System

In visual threshold, the fingerprint template is divided into N shares, N-1 is stored into the server and the one share is given to the users.

The overview of proposed work is shown in the figure-1. From figure-1, the original image (knuckle image) is taken as input image. In the next step, it will undergo for key point extraction using SIFT algorithm. In SIFT algorithm, it includes four steps. 1) Key point identification, 2) Key point localization, 3) Orientation process, 4) Key point Descriptor. In the step, it will undergo K-Means Algorithm to group the similar characteristic Key points at one place. Shamir Secret Sharing algorithm is used for division of Key points into n-parts that will be stored in the data server. It will undergo further four processes.

Process - 1 : It searches in data server and recreates the given image.
Process – 2 : From the process -1, key points were noted. Give the one more input image and it undergoes through process-1 and 2 again.
Process – 3 : Key points of two images were noted.
Process – 4 : If key points of two images were found matching, authentication occurs.

IV. RESULTS AND DISCUSSION

Fig.2 Input Image

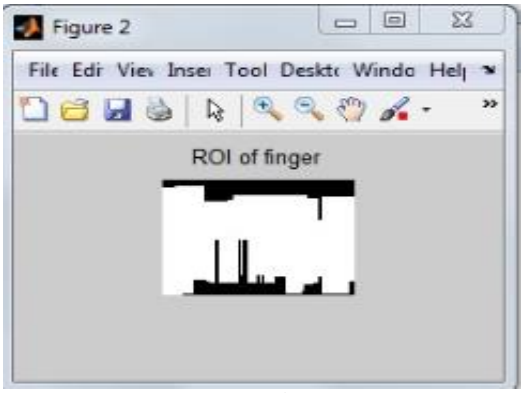


Fig.3 ROI of Finger

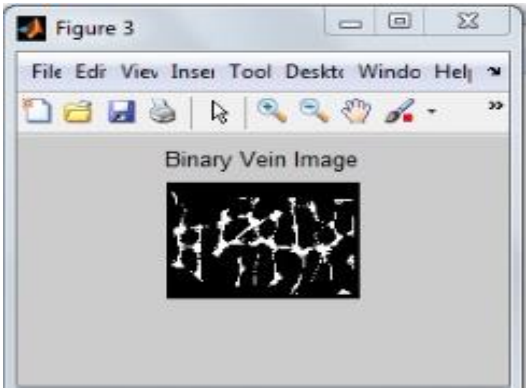


Fig.4 Binary Vein Image

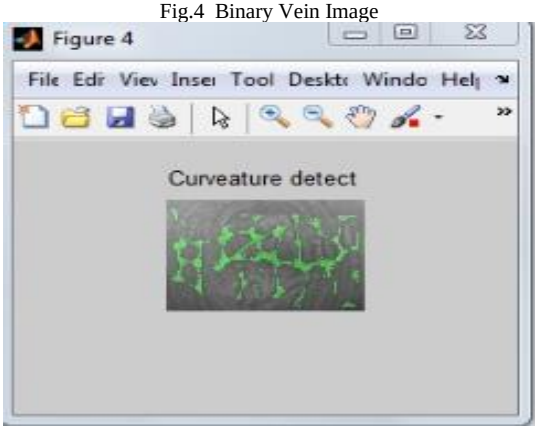


Fig.5 Curvature Detect

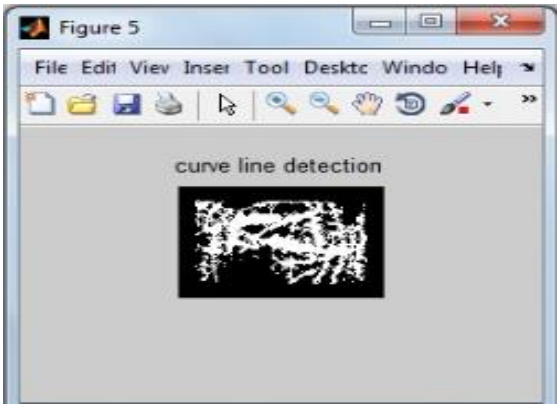


Fig.6 Curve Line Detection

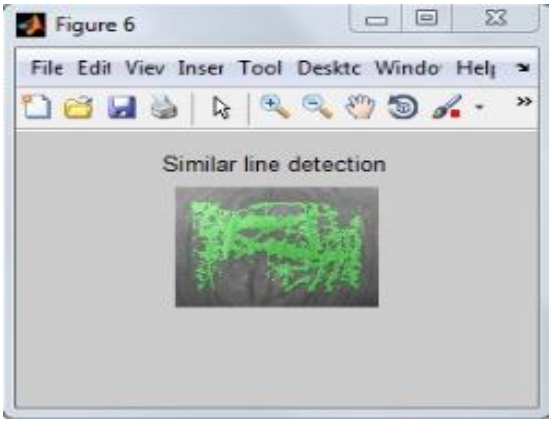


Fig.7 Similar Line Detection

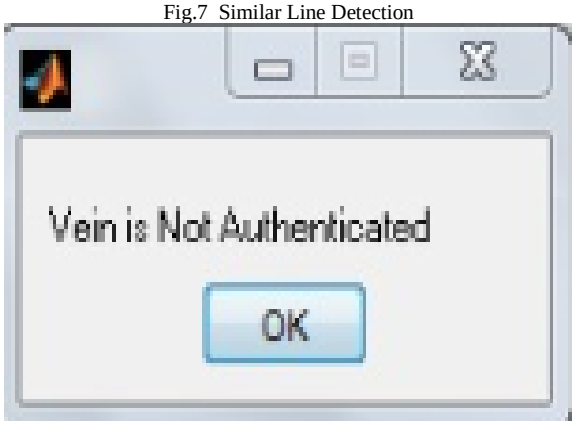


Fig.8 Vein is Not Authenticated

Shamir's Secret Sharing Algorithm: Shamir's Secret Sharing is an algorithm in cryptography created by Adi Shamir. The main aim of this algorithm is to divide secret that needs to be encrypted into various unique parts. As shown in fig.9

- Let's say **S** is the secret that we wish to encode.
- It is divided into N parts: S1, S2, S3, …., Sn.
- After dividing it, a number **K** is chosen by the user in order to decrypt the parts and find the original secret.
- It is chosen in such a way that if we know less than K parts, then we will not be able to find the secret S (i.e.) the secret S cannot be reconstructed with (K – 1) parts or fewer.
- If we know **K** or more parts from S1, S2, S3, …., Sn, then we can compute/reconstructed our secret code S easily. This is conventionally called (K, N) threshold scheme.

The main idea behind the Shamir's Secret Sharing Algorithm lies behind the concept that for the given K points we can find a polynomial equation with the degree (K – 1).

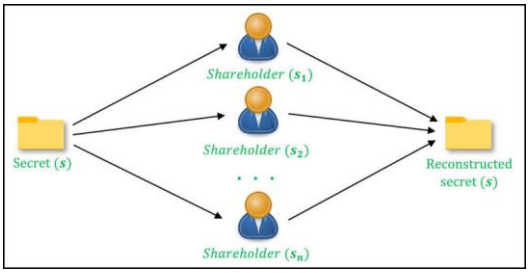


Fig.9 Shamir Secret Sharing Algorithm

SIFT Algorithm :
SIFT-Scale Invariant Feature Transform

There are some points on any object called as key points. These key points each other hold unique characteristics. These characteristics can be extracted from the object to provide complete description of an object. This helps to find the location of an object which consists of an image containing more objects. There are some rules to be followed while extracting key points from the object.

In larger images SIFT key points allow objects for multiple images at same location from the object to be recognised SIFT algorithm key points can be easily recovered from the effects of noise during extraction process.

Key point Detection
This is the first stage of Scale Invariant Feature Transform algorithm. This process is used to locate the edges of an image from different views of same object. It detects the each point from up to down and left to right of an object. This can be achieved by calculation of the Gaussian function. As shown in the below fig.10

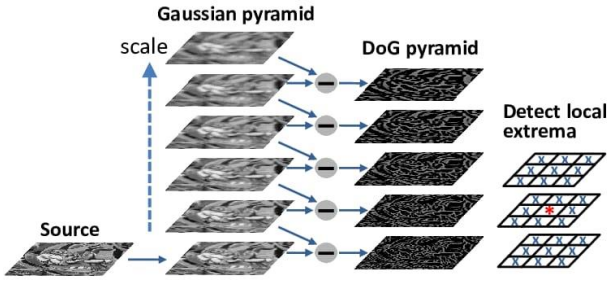
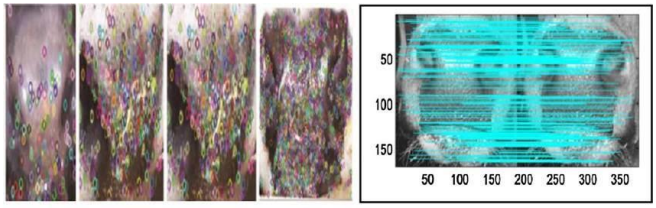


Fig.10 Key point Detection

Keypoint Localisation
This is the secondstage of Scale Invariant Feature Transform algorithm. This process used to remove the number of key points which have less difference in their characteristics. This can be achieved by calculation of the Laplacian function. As shown in the below fig.11



(a) (b)

Fig.11 Key point Localisation

Orientation Assignment

This is the third stage of Scale Invariant Feature Transform algorithm. The main aim of this step is to provide direction to the key points based on the image properties of the object. This process is used to find the direction of key points. Some points will be given of two or more directions. By using Gaussian key points of an image can be smoothed.

Keypoint Descriptor

This is the fourth stage of Scale Invariant Feature Transform algorithm. This process is used to assign a unique characteristics to each key point. These characteristics are used to create a set of histograms the gradient information can be used to find the direction of the key points. The weight of Gaussian is 1.5* key point scale. It consists of 16 histogram with 4x4 size each with 8 different directions. This results in over 128 elements. As shown in the below fig.12

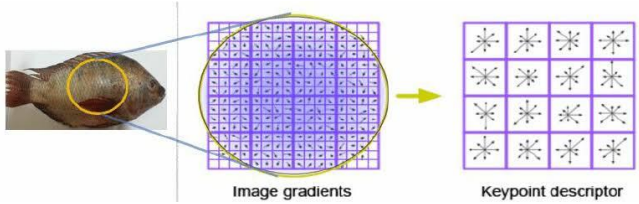


Fig.12 Key point Descriptor

K-MEANS Algorithm :

It is an iterative algorithm that divides the unlabeled dataset into n different groups in such a way that each dataset belongs only one group that has similar properties. Each data set has their own groups. It also divide each data set internally into groups. The distance between the data sets and groups centre should be minimum. There will be more similar data sets within a single group.

The K-means algorithm is as follows:

It is used to find out the number of groups n.

Shuffle the data sets of a group's n from the centre of data sets without any replacement.

Keep on repeating of assigning the values to data sets till there will be no change in centre.

Calculate the sum of distance between all data sets and all centres.

Find the closest centre and allot the each data set to it.

Find the average between the all data sets and all centres for all groups.

These are the some of important points to be noted:

- Calculate the values of the data sets for applying the K-means algorithm.
- Different method were used for finding the number of groups. But some of the methods won't work for finding the number of groups.
- This algorithm gives more weight to the bigger groups.
- This algorithm assumes that groups are in spherical type of shapes. These spherical shapes doesn't work for this types of groups. Elliptical type of shapes also doesn't work for this type of groups.
- If one group collide with another group, this algorithm doesn't have any measures for recovering the groups. This collision can't over come to find the which group is assigned to which data set.
- This algorithm can still divide the data sets without grouping the key points and distributes among itself. As shown in the below fig.13.

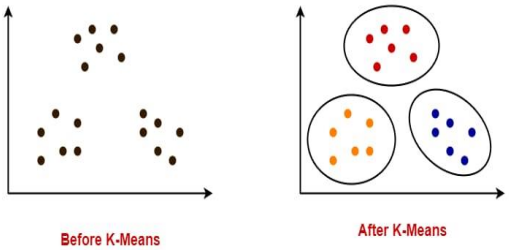


Fig.13 K-MEANS Algorithm

V. CONCLUSION:

This project follows a method of cryptographic techniques to the finger knuckle print extraction using visual threshold cryptographic techniques. In Accordance with the work done, the authentication and hiding could be completed. This method is secure against sever server attacks and data theft. Visual Threshold Cryptographic techniques divides the image into n parts it requires only n-1 parts for authentication. To improve the confidentialityeach part is stored into different servers, instead of storing the all parts into single server.

REFERENCES

[1] Noar M., Shamir A., 2017. Visual cryptography. Advances in Cryptography. Eurocrypt'94, Lecture Notes in Computer Science, vol. 950, Springer-Verlag. 1 – 12.

[2] Tsai C.S., Chang C.C., Chen T.S., 2016. Sharing multiple secrets in Digital images. Department of Computer Science and Information Engineering, Taiwan. 1 – 8.

[3] MuthukumarArunachalam and Kannan Subramanian, Department of Electronics and Communication Engineering, Kalasalingam University, India. The International Arab Journal of Information Technology, Vol. 12, No. 6A, 2015.

[4] Subba Rao Y.V., 2015. Presentation on Visual Cryptography and Its Applications. Department of Computer and Information Sciences, University of Hyderabad, India. 1 – 42.

[5] Jain A., Hong L., Pankanti S., Bolle R., 2015.An Identity Authentication System Using Fingerprints. Department of Computer Science, Michigan State University, USA. 1- 66.

[6] George A., "Efficient High Dimension Data Clustering usinConstraintPartitioning K-Means Algorithm," the International Arab Journal of Information Technology, vol. 10, no. 6, pp. 467-476, 2013.

[7] Bistarelli S.,Boffi G., Rossi F., 2012. Computer Algebra for Fingerprint Matching. Universita "G. d'Annunzio", Dipartimento di Scienze, Pescara, Italy. 1 – 10.

[8] Meskine F. and Bahloul S., "Privacy Preserving K-Means Clustering: A Survey Research," the International Arab Journal of Information Technology, vol. 9, no. 2, pp. 194-200, 2012.

[9] Zhang L., Zhang L., Zhang D., and Guo Z., "Phase Congruency Induced
Local Features for Finger-Knuckle-Print Recognition," Pattern Recognition, vol. 45, no. 7, pp. 2522-2531, 2012.

[10] Mahmud M., Khan M., Alghathbar K., Abdullah A., and Idris M., "Intrinsic Authentication of Multimedia Objects Using Biometric Data

Manipulation," the International Arab Journal of Information Technology, vol. 9, no. 4, pp. 336-342, 2012,.

[11] Qing L., "Finger Knuckle Print Recognition based on SUR Algorithm," in Proceedings of the 8th International Conference on Fuzzy Systems and Knowledge Discovery, Shanghai, pp.1879-1883, 2011.

[12] Wankou Y., Changyin S., and Zhongxi S., "Finger-Knuckle-Print Recognition Using Gabor Feature and OLDA," in Proceedings of the 30th Chinese Control Conference, Yantai, China, pp. 2975-2978, 2011.

[13]Stinson D.R.,Tavares S., 2010. The Pseudo-Random Number. Selected Areas in Cryptography. 7th Annual International Workshop, Waterloo, Ontario, Canada. 100 – 101

[14] Y.V. Subba Rao, Ms. YuliaSukonkina "Fingerprint based authentication application using visual cryptography methods (Improved ID card),' , IEEE TENCON 2008, pp 1-5.

[15] Davide Maltoni 2003. Handbook of Fingerprint Recognition. 1 – 366.