International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Articles available online http://www.ijoer.in; editorijoer@gmail.com

Vol.5., Issue.1., 2017
January-February

RESEARCH ARTICLE

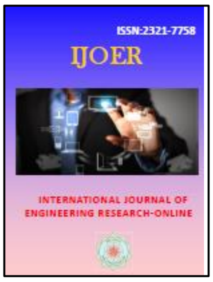
ISSN: 2321-7758

MIXED FINGERPRINT ENCRYPTION USING LFSR TO SECURE IMAGES

STEFFY LIVERA[1], SREELA SREEDHAR[2]

[1]MTech scholar, Computer Science Department , Toc H Institute of Science and Technolgy, Arakkunnam, Kochi , India, E-mail : 0stera0@gmail.com

[2]Associate Professor, Head of the Department., Computer Science , Toc H Institute of Science and Technology, Arakkunnam, Kochi , India, E-mail : sreelasreedhar@gmail.com



ABSTRACT

This paper, proposes a fingerprint based data encryption strategy to secure images. The attacker can track the fingerprints and use them for their purpose if they stole the database. Hence, to provide security to the fingerprint is important. To provide privacy protection to the fingerprints, system combines two fingerprints into a new virtual individuality. It further extracts the minutiae features from both the fingerprints and generates a mixed minutiae template. Mixed minutiae template is generated from the mixed fingerprints image. In Biometrics, this method can create a new identity of a person which provides more security. The new virtual fingerprint is used as they key for encrypting images. The decryption of the image has made difficult for the attackers and hijackers in such a way that decryption is possible only if one can have the combinations of the two fingerprints that have used in the process. The proposed system provides more security for the images.

Key Words - Cryptography, Decryption, Encryption, Fingerprint Image, Minutiae position, Mixed Fingerprint, Orientation estimation.

I.INTRODUCTION

Biometrics methods like palm print, finger print, iris, signature, retina, and face are widely being used in personnel identification systems and the fingerprint based identification is used even in ancient times. A fingerprint is made of a series of ridges and furrows on the surface of the finger. The uniqueness of a fingerprint can be determined by the pattern of ridges and furrows as well as the minutiae points [1]. Fingerprints are unique for individuals and across different fingers of the same individual. The minutiae are the unique features of fingerprints, which involve the position, direction and type, etc. The distribution of minutiae can classify fingerprints into whorls, loops and arches [2]. A fingerprint is the feature pattern of one finger [3]. Each person has his own fingerprints with the permanent uniqueness. However, shown by intensive research fingerprint recognition, fingerprints are not distinguished by their ridges and furrows, but by minutiae. Biometric systems are gaining reputation as more reliable alternatives to password based security systems, as they do not necessitate passwords to be remembered and biometrics are intricate to be copied and free of thefts. Moreover, biometrics offers non-repudiation (an authenticated user cannot deny having done so) to some extent owing to the intricacy in copying or stealing individual's biometrics.

Cryptography is defined as the art and science of generating secret messages. An original plaintext is coded into the cipher text through the process of encryption and the plaintext is restored from the cipher text through the process of decryption. The many schemes used for encryption constitute the area of study known as cryptography. Cryptanalysis is "Breaking the code" without the knowledge of any encryption techniques. The areas of cryptography and cryptanalysis together are called cryptology [4].

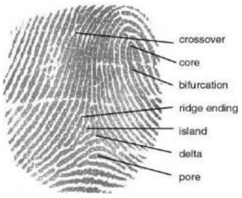


Fig. 1. Fingerprint Structure

Cryptography, is concerned with the projection of trust with transferring trust from where it exists to where it is necessitated [5]. The strength of the cryptographic algorithms depends on the length of the key employed. Although keys of significant length are strong against both brute force and factorization attacks, they still suffer from some inherent weaknesses. For decades, the prime factor limiting the security of systems is the inability of human users to bear strong cryptographic keys in mind. The past records have demonstrated that users cannot remember long passwords, and in addition they tend to prefer passwords that are effortlessly attacked by dictionary attacks. The above limitation could be overcome in an extensive range of applications by producing strong cryptographic keys from biometric data[6],[7],[8].

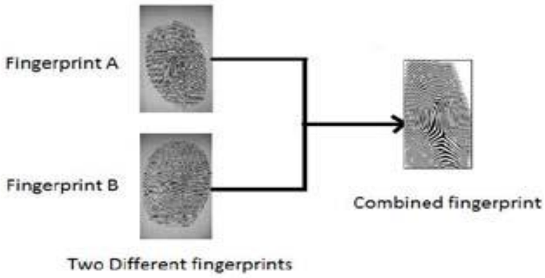


Fig. 2. Combined Fingerprint from two different fingerprints

Image protection is transforming the image into a new format which is completely different from its original format. It must be hard to understand its design in such a way to keep the image confidential between the users by using an effective approach called image encryption, which is essential that nobody could get to know the content of new image without a key to reconstruct the original image, this process of reconstruction of the image is called decryption [9].

II.VIRTUAL FINGERPRINT CREATION

To produce privacy protection to the fingerprints system combines the two completely different fingerprints into a brand new virtual identity. And additional extracts the trivialities options from each the fingerprints and generates a combined trivialities template [10].The assaulter cannot distinguish the initial fingerprint from combined fingerprint. Therefore, combined fingerprint system generates a combined fingerprint to guard privacy of fingerprints. Fig. 1. shows generated combined fingerprint from completely different fingerprint pictures.

A. *Combined Fingerprint System*

The Fig. 3. offers the combined fingerprint system. It takes completely different fingerprints for enrollment part then enhances those fingerprints. It extracts the trivia point's type thumbprint A and position from thumbprint B and each from reference. For authentication part, taking fingerprints, once more doing the same procedure for extracting the combined trivia points for these fingerprints is dispensed. Then examination of these trivia examples with template will keep within the information. The match is checked to attest or to discard [11].

B. *Combined Fingerprint Image Generation*

Once combining fingerprint generation extracts the combined trivia template and can be hold on in very information for the match images which needs both question thumbprints. A two-layer thumbprint compare method matches the both question thumbprint against a mixed trivia example. Extract the options of each mixed trivia example that is hold on in very information and therefore the question trivia template. Then match these options and calculate the matching score between them. If the score is higher than the brink, then fingerprints are matched which allows authentication otherwise not.

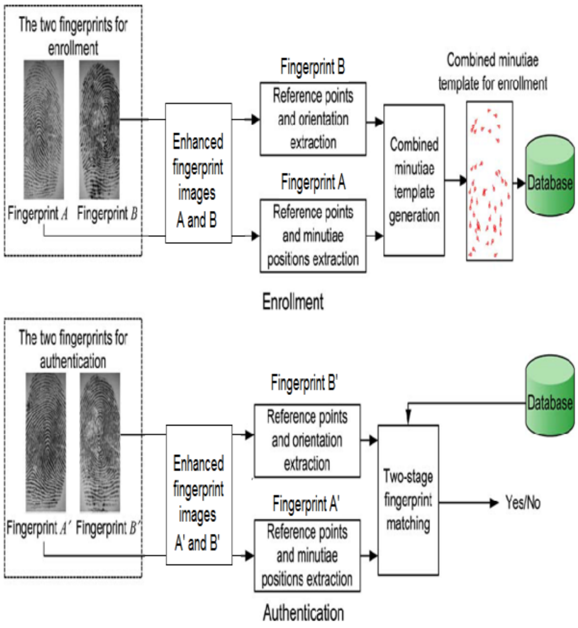

The two fingerprints for enrollment
Fingerprint A
Fingerprint B
Enhanced fingerprint images A and B
Fingerprint B
Reference points and orientation extraction
Fingerprint A
Reference points and minutiae positions extraction
Combined minutiae template generation
Combined minutiae template for enrollment
Database
Enrollment
The two fingerprints for authentication
Fingerprint A'
Fingerprint B'
Enhanced fingerprint images A' and B'
Fingerprint B'
Reference points and orientation extraction
Fingerprint A'
Reference points and minutiae positions extraction
Two-stage fingerprint matching
Database
Yes/No
Authentication

Fig. 3. Combined Fingerprint System

This method [4] protects the privacy of fingerprints and generates a brand new identity of a combined fingerprint. a way to extract the trivia points from the skinny fingerprint image. The preprocessing steps are needed to extract the options from a fingerprint image, then once obtaining skinny image extract the trivia points and orientations. Then generates the combined fingerprint image and extract the combined trivia template. For authentication, extract the question trivia template from two question fingerprints and match with the template holds on into the information. If match found, then certify it otherwise not [12]. The mixed thumbprint image is generated from two different fingerprint image in which proposed system takes minutiae points from 1st fingerprint and orientations from 2nd fingerprint and reference points for both.

There are 7 stages to generate combined fingerprint image as follows [4]:

1. Estimate associate degree orientation from the set of trivialities points by acceptance the position regenerating algorithmic rule.
2. Generate a binary ridge pattern based on *O* and a predefined fingerprint ridge frequency using Gabor filters.
3. Calculate the section of image of the binary shape pattern victimization the thumbprint FM-AM model.
4. Regenerate the continuous phase image by reduces the spirals in the image.
5. Mix the continual part image and also the spiral part image, manufacturing a reconstructed part image.
6. Produce a refined phase image from regenerated phase image by removing spurious minutiae points.
7. Apply an unwanted noise and rendering step refined image, thus on produce a original look like thumbprint image. To generate a mixed thumbprint, estimate the orientation field form set of small points by using the algorithm proposed in.

C. Mixed Minutiae Template Generation

The mixed minutiae template is produced from the combination of minutiae points of the first fingerprint and orientation of the second fingerprint.

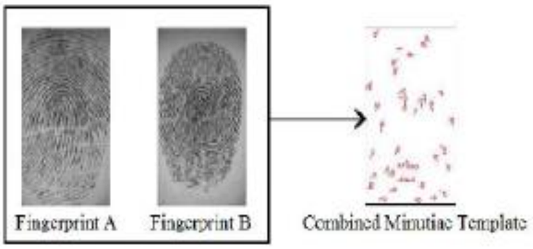


Fig. 4. Combined Minutiae Template from Two Different Fingerprints

D. Architecture of Fingerprint System

The minutiae points are calculated during the enrolment phase and it is stored in the database. The minutiae points will be calculated again during the log in time and it is compared with the stored minutiae points in the database to identify whether the user is authenticated. In the enrolment phase, two distinct fingerprint images of A & B are taken and it is enhanced to gray level image. From the gray level images, extract the minutiae points from the two distinct fingerprint images and create a combined minutiae template and store the minutiae points from the minutiae template to the database. In the matching phase, two distinct fingerprint images of A and B are taken and it is enhanced to gray level image. From the gray level images, extract the minutiae points from the two distinct fingerprint images and create a combined minutiae template and it is compared with the stored minutiae points in the database and checks whether it is matching.

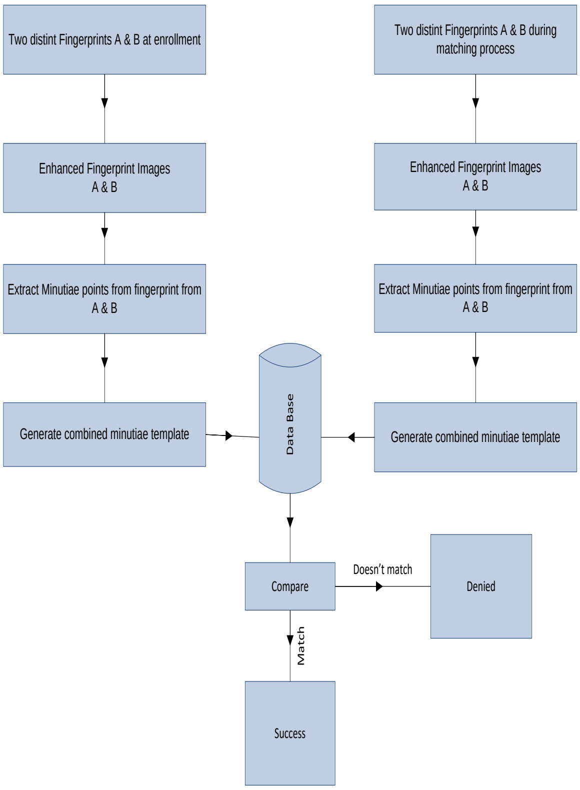

Two distint Fingerprints A & B at enrollment
Two distint Fingerprints A & B during matching process
Enhanced Fingerprint Images A & B
Enhanced Fingerprint Images A & B
Extract Minutiae points from fingerprint from A & B
Extract Minutiae points from fingerprint from A & B
Data Base
Generate combined minutiae template
Generate combined minutiae template
Compare
Doesn't match
Denied
Match
Success

Fig. 5. Architecture of Fingerprint System

III.DIGITAL IMAGE PROCESSING

An image may be defined as a two dimensional function f(x,y) , where x and y are spatial (plane) coordinates, and the amplitude off at any pair of coordinates (x, y) is called the intensity or gray level of the image at that point. When x, y, and the intensity values of f are all finite, discrete quantities, we call the image a digital image. The field of digital image processing refers to processing digital images by means of a digital computer. A digital image is composed of a finite number of elements, each of which has a particular location and value. These elements are called picture elements, image elements, pels, and pixels. Pixel is the term used most widely to denote the elements of a digital image. An image file for a computer can simply be regarded as a file having multiple colors and different light intensities on different areas of the image. An image thus can be represented as a collection of pixels stored in a tabular form, generally in a matrix therefore helps in processing the image easily. If we consider an image having "i" pixels in the horizontal direction and "j" pixels in the vertical direction, then the total number of pixels in the mage would be [i*j] and this value is also known as the size of the image. Further each pixel value of an image to be stored, can be represented as a collection of bits. As far as grey scale images are considered the number of bits required to represent a pixel is 8. The reason being, in grey scale images the color intensity of a particular pixel will vary from 0 to 255 where the value "0" corresponds to black and the value "255" corresponds to white. This means that the maximum value a pixel could have is 255 and therefore 8 bits are required. A colored image on the other hand is made up of pixels, each comprising of three color components, these being red, green and blue component. The colour intensity of the pixel will depend on the proportion of these three components. Now in order to represent each colour component 8 bits are required 203 which means that, in order to store each pixel of a coloured image 24 bits are used.

A. Encrypting Image File Using Virtual Fingerprint

In the proposed system, the templates of two fingerprints are taken and a combined fingerprint is generated. This is used as the key for the encryption algorithm, which results in the strong encryption. The process of reverting ciphertext to its original plaintext is called decryption.

Algorithm for encryption : The first step in this phase is to load the colour image that is intended to be encrypted using new virtual fingerprint to LFSRs that will generate random numbers to reorder position of each pixels in the row of image in the first encryption process. The second encryption process gives the virtual fingerprint to generate a new random numbers used to reorder position of pixels in each column in the resulting image of the first encryption process.

The main steps of our proposed method to encrypt image are:

1. Input color image

2. Giving minutiae points of virtual fingerprint to LFSRs
3. Generating a random numbers for each row in the image
4. Encrypting the image
5. Again minutiae points of virtual fingerprint is given to the LFSRs.
6. Generating a random numbers for each column in the encrypted image
7. Encrypting the image
8. Applied XOR
9. Save encrypted image

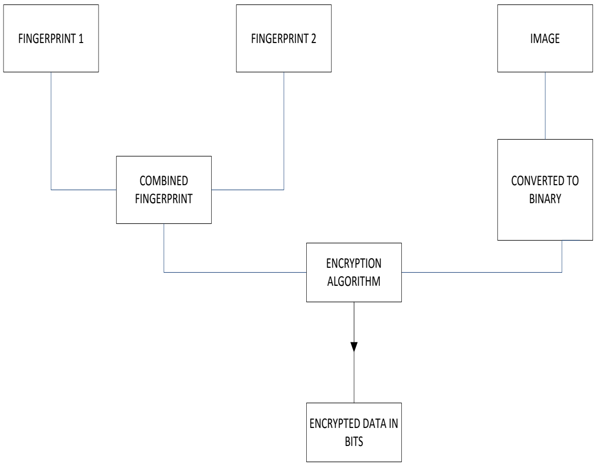


Fig.6. Encryption process

Algorithm for decryption : The first step in decryption phase is to load encryption colour image that is intended to be decrypted by using the same virtual fingerprint in the LFSRs to generate the same random number to decrypt the image with column and row process.

The main steps of our proposed method algorithm to decrypt image are:

1. Input encrypted color image
2. Applied XOR
3. Giving the virtual fingerprint image to LFSRs
4. Generating a random numbers for each column in the encrypted image
5. Decrypting the image
6. Giving virtual fingerprint to the LFSRs.
7. Generating a random numbers for each row in the encrypted image
8. Decrypting the image
9. Original image is displayed

IV.CONCLUSION

Image protection is transformed it into new format different completely from its original format that is hard to understand. To keep the image confidential between users by using an effective approach called image encryption, is essential that nobody could get to know the content of new image without a key to reconstructed the original image, this process of reconstructed the image is called decryption. To provide privacy protection to the fingerprints, system combines two distinct fingerprints into a new virtual individuality. It further extracts the minutiae features from both the thumbprints and generates a mixed minutiae template. Mixed minutiae template is generated from the mixed thumbprint images. This new virtual identity is used as the key for the image encryption and decryption which provides tight security to the original image since the key for the algorithm requires the physical presence of the individual.

References

[1] H. Chen,H.Chen, “A novel algorithm of fingerprint encryption using minutiae based transformation”, Pattern Recognit. Lett.32(2)(2011) 305–309.

[2] Lee, H. C. and Gaensslen, R.E., 1991. “Advance in fingerprint technology”, Elsevier, New York

[3] P. Komarinski, P. T. Higgins, and K. M. Higgins, K. Fox Lisa, “Automated Fingerprint Identification Systems (AFIS)”, Elsevier Academic Press, pp. 1-118, 2005.

[4] Prashant Bhaskarrao Patil, Nitin N. Patil, “Effect of Algorithms for the Extraction of Minutiae Position and Orientation in Thumbprint Mixing” , 2016 International Conference on Computer Communication and Informatics (ICCCI -2016), Jan. 07 – 09, 2016, Coimbatore, INDIA.

[5] Feng Hao, Ross Anderson, John Daugman, "Combining cryptography with biometrics effectively", Technical Report, 2005.

[6] A. Juels and M. Wattenberg, “ A fuzzy commitment scheme”, In Proceedings of the 6th ACM Conference on Computer and Communication Security, pp: 28–36, November 1999.

[7] F. Monrose, M. K. Reiter, and S. Wetzel, “Password hardening based on key stroke dynamics”, In Proceedings of the 6th ACM

Conference on Computer and Communications Security, pages 73–82, November 1999.

[8] Chen, B. and Chandran, V., "Biometric Based Cryptographic Key Generation from Faces," 9th Biennial Conference of the Australian Pattern Recognition Society on Digital Image Computing Techniques and Applications, pp: 394 - 401, 3-5 Dec, 2007.

[9] Anurag S.,and Namrata D., " DIP Using Image Encryption and XOR Operation Affine Transform ",IOSR Journal of Computer Engineering (IOSR-JCE) ,Vol. 17, Issue 2, PP 07-15 , 2015.

[10] Sheng Li and Alex C. Kot, "Fingerprint Combination for Privacy Protection," IEEE Trans. on Information Forensics and Security, vol. 8, NO. 2, Feb. 2013.

[11] A. Ross and A. Othman, "Mixing fingerprints for template security and privacy," *in Proc. 19th Eur.Signal*, Barcelona, Spain, Aug. 29–Sep. 2, 2011.

[12] A.Othman and A. Ross, "Mixing fingerprints for generating virtual identities," *in Proc. IEEE Int.Workshop on Inform. Forensics and Security*, Brazil, Nov. 29–Dec. 2, 2011.

[13] Anurag S.,and Namrata D., " DIP Using Image Encryption and XOR Operation Affine Transform "IOSR Journal of Computer Engineering (IOSR-JCE) , Vol. 17, Issue 2, PP 07-15 , 2015.