International Conference on Emerging Innovation in Engineering and Technology

ICEIET-2017

A Survey On Lossless Compression And Encryption Methods For Multi Biometric Traits

Hemapriya.M[1], Ezhilarasan.M[2]
[1]M.Tech Student, [2]Professor, Information Technology
Priyamayaraman93@gmail.com

Abstract

This paper concentrates on comparative studying of existing lossless compression methods for biometric traits.The main contribution of this work is to provide a new approach which exploits the structura1 properties of fingerprint images to achieve higher lossless compression ratios and good qua1ity images. A natural result of this approach is that the original structural properties such as the number arid relative locations of ridge endings and bifurcations are well preserved i.e., they are not affected by reconstruction quality. They can be easily extracted from compressed data without reconstruction. Ten fingerprints and two iris images are been captured from their respective devices. Fingerprints are been preprocessed and then subjected to feature extraction process. In feature extraction process unwanted parts are removed. This process involves gray scale conversion, Resize, Histogram Equalization, canny edge detection. Compression is done to the output obtained from feature extraction module. Encryption is done to provide higher level security as data are used for authentication purpose.

Keywords— AES, Fingerprint, Iris, Minutia, RLE

I. INTRODUCTION

Biometrics refers the identification of a person based on their physical and behavioral characteristics. These characteristics include the traits like fingerprints, iris face, hand geometry, palm print, voice, signature, tongue, lips, sclera and knuckle. These biometrics features can be used for authentication purpose in e-passports, border control, biometric attendance, forensic, smart cards, driving license and Aadhar card. The ID cards, UID no, punch card, secret password and PIN are generally used for personal identification but they can be stolen easily. Passwords can be forgotten or even cracked. The biometric identification overcomes all the issues and it provides additional security among all other techniques; fingerprint recognition is the most popular method and is successfully used in many applications.

Fig. 1. Fingerprint

A fingerprint consists of several feature vectors to be taken into consideration. Ridges are present at the upper layer and valleys are placed at lower side. The ridges form the minutia points. Ridges can be placed under different structures such as ridge endings (the point where ridge end) and ridge bifurcations (splitting point of line). Many types of minutiae exist, which includes dots (very small ridges), islands (dots look as clusters), ponds or lakes (empty spaces between two temporarily divergent ridge or empty space surrounded by ridge), spurs (a notch protruding from the ridge), bridges (small ridges joining two adjacent ridges), and crossovers (two ridges which cross each other) [1]. The need for fingerprint compression is to deal with huge fingerprint database and it plays major role in many governments sector applications.

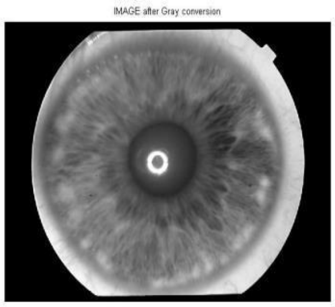

Fig. 2. Iris

Iris is a kind of physiological biometric trait. It contains unique texture and it is complex enough to be used as a biometric signature for authentication purpose. Compared with other biometric features such as hand geometry and fingerprint, iris patterns are more permanence and reliability. The intimacy level is very high and cannot be stolen without the knowledge of candidate. It is unique to people and stable with age. Iris recognition systems can be non-invasive to their users. It is impossible to duplicate iris patterns. The iris is a strong contender alongside face and fingerprints of inclusion in multimodal recognition systems. Multimodal biometric system will provide high level of authenticity and de duplication of all the biometric inputs of a candidate is very hardly feasible. Thus the proposed system will make use of ten fingerprints and two iris codes.

Cryptography is being used worldwide extensively for protecting information. The process of protecting information or image by encrypting it into an illegible format is called as cipher text. Merely people who hold the secret key can decipher the encipher data into original text. Remembering the key is very tedious task, due to the usage of 128,192 and 256 key bits. To solve this issue, biometrics can be used as a key. This increases the complexity of guessing and cracking a cryptographic key. Mixed key will provide better opinion for information security. Biometric key are been mixed with binding key in random for high efficiency.

The need for fingerprint and iris image compressed has been discussed in this section along with methods involved in it. Metrics and terminologies studied has been given in section II. Brief investigation of compression and encryption algorithms for various traits are described in section III. Conclusion of the analysis is done at section IV.

II. RELATED WORK

Compression of fingerprints is very crucial step in automated fingerprint identification systems due to the increasing number of the fingerprint records in their databases. Repeatedly compressing and decompression of a image will end up with reduction of quality. To attain superior compression ratios, standard structure of fingerprint images should be utilized. Classifications of fingerprint compression techniques fall under two divisions they are: 1) fingerprint data compression technique: It is based on extracting and compressing of feature vectors such as ridges and/or other vectors. 2) Fingerprint image compression technique: It is based on image transforms and does not make use of regular structural properties.

The iris image is cropped and resized from its standard format, the part containing iris is alone cropped. Eye finding algorithm is used to do this process [2]. Further it is been applied with JPEG compression. There are several scalar and vector quantization methods used for fingerprint compression. U.S government has implemented new digital image compression standard in F.B.I. It is based on adaptive scalar quantization method and DWT. Lattice vector quantization method is used for achieving high compression ratio [3].

Compression size
It is the size of new file achieved after applying compression technique [4].

Compression ratio
It is the result obtained from dividing size of compressed file by size of uncompressed file and multiplying the value with hundred.

Compression time
It is the actual Time taken to compress the original file or number of files compressed per millisecond. The compression and decompression time of the algorithm should be up to the acceptable level [5].

Histogram equalization
The process is done in order to enlarge the pixel value circulation of an image so as to increase the perceptional data. The original histogram of a fingerprint image has the bimodal type, the result obtained after the histogram equalization occupies the range 0-255 and the visualization effect is also enhanced finally [6].

Binarization
Fingerprint Image Binarization is to transform the eight bit Gray fingerprint image into bit values of 0&1. After the operation, ridges in the fingerprint are tinted with black color while furrows are colored in white. A locally adaptive binarization technique is carried out to binarize the biometric trait.

III. LITERATURE SURVEY

The following description is about my analysis on papers I had taken under consideration.

In [7], a model based approach for compression of fingerprints was proposed. They reconstruct the image from ridge pattern obtained and it creates the sparse representation. Reconstruction is done using an hybrid image model. There is no modification or missing of pixel in the reconstructed image as it depends on permanent ridge structure. Differential chain codes plays prominent role in coding efficiency. The limitation of this system is that overall course of action involves many iterations and it becomes bottleneck for decompression stage.

In [8], they have described about sampling and compressing of human iris. The resilience of identity verification systems have been tested for three sky-scraping performance iris matching algorithms. The images are resized an sampling is done by their Fourier coefficients. Texture is been maintained even after noise reduction task. Compression ratio obtained by this process results good for smaller file size. Demerit of this system is it should preserve 99% image power radically but sub sampling studies report that it is not sufficient; therefore system does not provide a level playing field for evaluation.

In [9], three methods for compression of iris had been investigated in order to assess what their impact would be on recognition performance of the algorithm deployed for authenticating and indentifying people by their biometric traits. Standard iris images are six hundred times larger than iris template. There is an no exception administratively the iris image should be stored, transmitted and embedded in the form of images rather than templates that are computed with proprietary algorithms. To achieve the goal of bandwidth and storage implications we can combine ROI with JPEG compression at several stages. We can even test them on publically available iris image databases. The main drawback of the system is cropping leads to hamming distance error.

In [10], a generic fingerprint image compression technique based on wave atoms decomposition was proposed. Multi resolution analysis tools have been successfully applied for fingerprint image compression for more than a decade. Wave atoms decomposition has specifically been designed for enhanced representation of oscillatory patterns to convey temporal and spatial information. Our proposed compression scheme is based upon linear vector quantization of decomposed wave atoms representation of fingerprint images. Later quantized information is encoded with arithmetic entropy scheme. The proposed image compression standard outperforms the FBI fingerprint image compression standard, the wavelet scalar quantization (WSQ). The quality of various image compression techniques depends upon how close is the reconstructed image to the original image. Different metrics are proposed for investigating the quality of compression algorithms. Some methods investigate similarity while others explore the level of dissimilarity between reconstructed and the reference image. Mean square error (MSE) and peak signal to noise ratio (PSNR) are two celebrated metrics used to examine the qualitative performance. Limitation of this system is quality is highly affected.

In [11], a new method that combines arithmetic coding with Run length encoding (RLE) for lossless image compression was proposed. Run length encoding is used to reduce size by removing unwanted pixels in the image and avoid repetition of same pixel value which would lead to higher size. Results obtained from this proposed system is lossless compression is suitable for both static and adaptive model. Limitations are quality and compression ratio. Quality of decompressed image is hardly feasible.

In [12], a survey on biometric cryptosystem and cancelable biometrics was proposed. It makes use of AES algorithm and biometric salting method. Form a privacy perspective most concerns against the common use of biometrics arise from the storage and misuse of biometric data. Biometric cryptosystems and cancelable biometrics represent emerging technologies of biometric template protection addressing these concerns and improving public confidence and acceptance of biometrics. In addition, biometric cryptosystems provide mechanisms for biometric-dependent key-release. In the last years a significant amount of approaches to both technologies have been published. A comprehensive survey of biometric cryptosystems and cancelable biometrics is presented. State-of-the-art approaches are reviewed based on in-depth discussion. Demerit of this system are practical recognition rate should be increased and stolen token scenario.

In [13], IRIS Authentication Based on AES Algorithm was proposed. Cryptosystem is widely used in many information security application were the identification and verification are done by passwords, pin number etc which is easily cracked by others. So biometric cryptosystem is a powerful unique tool based on the anatomical and behavioral characteristics of the human beings in order to proof the authentication. Iris is used for generation of 128 bit binary. Extracting the multiple iris features from local iris image is based on Independent Component Analysis (ICA) to reduce the dimensionality and to get accurate iris feature vector. It is clustered and its centroid value is converted into 128 bits iris key using K-Means clustering. The clustering is used to minimize the intra variation on the extracted iris feature vector. This paper also proposes biometric cryptosystem based on AES encryption and decryption to protect the confidential information by using iris as a biometric key. CRC is used to check whether there is no modification in the original data. The advantages of this system are AES algorithm is very difficult to crack and is well suitable to security application and it has better resistance. AES is so simple and it had implemented easily.CRC had checked the message and give a genuine and imposter.

In [14], diagnostically lossless coding of X-ray angiography images based on background suppression was proposed. Diagnostically lossless coding algorithm is been used. Advantage of the system is it achieves 0.98% better results when compared to manual segmentation. Disadvantage of this system is lower compression ratio.

IV. CONCLUSION

This paper shows the comparison of different lossless compression algorithms for biometric traits such as fingerprint and iris and encryption methods which are used as on date. By considering the compression time and compression ratio of all the algorithms it's clearly known that reconstruction and sub sampling should be concentrated to achieve higher quality. Reconstruction of image from ridge structure is very hardly feasible with few complications, so fingerprint image can be considered for better results. Segmentation also plays major role in achieving quality. AES algorithm is very difficult to crack and is well suitable to security application and it has better resistance. AES is so simple and it can be implemented easily.CRC had checked the message and give a genuine and imposter.

REFERENCES

[1]G Arunalatha and M. Ezhilarasan "A Review on Fingerprint Image Compression", I J I T E no. 3, pp. 179-185, 2012.

[2] John Daugman and Cathryn Downing "Effect of Severe Image Compression on Iris Recognition Performance", *IEEE transactions on information forensics and security,* vol. 3, no. 1, pp. 52-61, 2008. Amit Jain, Kamaljit I, Lakhtaria, Prateek Srivastava "A Comparative Study of Lossless Compression algorithm on Text Data", *Elsevier Science Direct, Advances in Computer Science*, pp. 536-543, 2013.

[3]Saravanan S, Sanjeev S malalur and Micahel T Manry "Fingerprint Feature Compression Using Statistical Coding Techniques", *Proc. IEEE Annual India Conference, (INDICON),* pp. 1–4, 2009.

[5] R. Jubiya, M. Keirthi, M. Anupriya and A. Muthukumar "IRIS Authentication Based On AES Algorithm", *International Journal of Innovative Research in Science, Engineering and Technology*, Volume 3, Special Issue 3, March 2014.

[6] Soni Prattipati1, M. N. S. Swamy and Pramod K. Meher "A Comparison of Integer Cosine and Tchebichef Transforms for Image Compression Using Variable Quantization", *Journal of Signal and Information Processing*, vol 6, pp. 203-216, 2015.

[7] Ilker Ersoy and Fikret ETC Muhittin Gokmen "A Model-Based Approach for Compression of Fingerprint images", *Proc.IEEE Image Processing*, 2, pp. 973-977, 1999.

[8] Soumyadip Rakshit and Donald M Manora "An Evaluation of image sampling and compression for human iris recognition", *IEEE transactions on information forensics and security,* vol. 2, no.3, pp. 605-612, 2007.

[9]Nanunzhou, Shumin and Shan Cheng "Image compression-encryption scheme based on hyper-chotic system and 2D", *Elsevier Science Direct, optics & Laser Technology,* pp. 121-133, 2016.

[10] Abdul A. Mohammed, Rashid Minhas, Q. M. Jonathan Wu, Maher A and Sid-Ahmed "Fingerprint Image Compression Standard Based On Wave Atoms Decomposition and Self Organizing feature map", *Proc. IEEE, Electro/Information Technology*, pp.367–372, 2009.

[11] Med Karim Abdmouleh, Atef Masmoudi and Med Salim Bouhlel "A new method which combines arithmetic coding with RLE for lossless image compression" *Science Research*, *Journal of software engineering and Applications,* pp.41-44, 2012.

[12] Christian Rathgeb and Andreas Uhl "A survey on biometric cryptosystem and cancelable biometrics", Springer*, Journal on Information Security,* 2013.

[13] S. Sridevi Sathya Priya and P. Karthigaikumar "Mixed Random 128

Bit Key Using Finger Print Features and Binding Key for AES

Algorithm", *International Conference on Contemporary Computing and Informatics,* 2014.

[14] Zhongwei Xu a, Joan Bartrina-Rapesta , Ian Blanes a , Victor Sanchez b , Joan Serra-Sagristàa , Marcel García-Bach and Juan Francisco Muñoz "Diagnostically lossless coding of X-ray angiography images based on background suppression", *Elsevier Science Direct, computers and Electrical Engineering,* pp. 1-14, Feb. 2016