IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

Improving Iris Recognition Performance by Using Cryptography

Pooja[1], R. M. Potdar[2]

M.Tech, Research Scholar, Department of ET&T, Bhilai Institute of Technology, Durg, India[1]

Associate Professor, Department of ET&T, Bhilai Institute of Technology, Durg, India[2]

Abstract: Various aspects of existence area unit step by step being digitized as our life experiences and inventive effort area unit accumulate in personal computers digital media devices and mobile devices. Folks use password and different authentication strategies to shield these collections of private and probably tip. Ancient strategies (e.g., personal passwords) area unit but secure. But these issues are often resolving through the "physiological passwords" through distinctive personal identification technique. There area unit numerous identification has been accustomed known the individual like face recognition, personal signature or iris recognition. Among of these statistics iris recognition is that the best biometric recognition for individual. Iris is extremely correct and reliable of their stable characteristics throughout lifespan. During this paper we have a tendency to improve the iris recognition performance by victimisation cryptography. Cryptography is that the technique that has a lot of security to the info or feature primarily based templates. In cryptography technique it'll be cipher the initial information of the iris that area unit supported the various options of the iris and at the last within the result half it'll be rewrite the initial information. Fuzzy commitment theme (FCS) is additionally introduced during this projected technique. It'll offer the correctness of the iris feature extraction and conjointly cut back the noise and error that area unit manufacture by the various angle of iris pictures. Thus during this paper we have a tendency to mentioned regarding the biometric recognition by victimization-on cryptosystem to boost the performance of iris recognition. Cryptosystem is nothing however it's the system that's victimisation the technique of cryptography meaning secret writing.

Keywords: Biometric, FCS, Physiological passwords, cryptography, cryptosystem, security, iris recognition.

I. INTRODUCTION

Nowadays, for providing the secure facilities and services to the user the proper identification is vital. Collectively in Associate in Nursing passing progressive digital society for secure identification has semiconductor to amplified development of biometric systems. The demand for such biometric system has increased dramatically because of the actual fact that such system acknowledges distinctive choices possessed by each individual. Iris recognition is that the most effective identification of individual. Iris recognition is extremely correct and reliable of their stable characteristics throughout amount of your time. Iris of each eye is exclusive. No a pair of irises unit of measurement alike in their mathematical detail even between identical twins and triplets or between one's Own left and right eyes. The iris remains stable throughout one's amount of your time, barring, rare malady or trauma. The random patterns of the iris unit of measurement the equivalent of a flowery "human barcode" created by a tangled textile on tissue and different visible choices. Biometric cryptosystems provide associate innovative resolution for bailiwick key generation, cryptography in additions biometric cryptosystems, original templates unit of measurement replaced by biometric dependent information that assists in sick is performed indirectly by corroborative the validity of recovered keys. A typical biometric primarily based authentication system consists of two methodology (i) the registration methodology, throughout that the system scans a users biometric image, creates a biometric model of biometric choices extracted from the image and hold on the model in knowledgebase's; and (ii) the authentication methodology, throughout that the system scans associate individual's biometric data, extracts biometric choices inside identical manner and compares them with the model of the user the individual claims to be. The system will output a match if in line with predefined similarity measure; a matter is sufficiently reasonably just like the model or a try if it isn't. However, widespread applications of bioscience have junction rectifier to new security challenges. As biometric templates unit of measurement physically hold on in databases or servers, presently photos unit of measurement able to be reconstructed once the templates unit of measurement compromised by attackers. Over the past few years, there has been a decent deal of labour on the thanks to defend biometric templates primarily, biometric protection technique use remodelled information instead of original biometric information or feature primarily based templates to manifest users. The foremost necessary aim of this biometric cryptosystem is to supply the high level of security of the model feature that unit of measurement store at intervals the data. In most existing work various iris recognition techniques has been utilized by pattern wholly totally different algorithmic program or together cryptosystem. In previous paper [1], Hindu deity madhuri.k, Viraj thakur, Rajesh jaiswal, Sandesh sonawane, Rohit nalavade, presented a biometric information security pattern recursive visual cryptography. They were primarily targeted on the technique of visual

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

cryptography. It's one all told the best best-known techniques to defend information like photos. presently [2] Cai Li, Jiankun Hu, Josef pieprzyk, Willy susilo given a latest bio cryptosystem sure security analysis framework and implementation of multi-biometric cryptosystem supported decision level fusion. Throughout this paper they deal with the multi-biometric cryptosystem in place of single biometric as a result of it provides stronger security and better authentication result.

[3] Dodis et al. projected a cryptographically key generation mechanism observed as fuzzy extractors. This methodology uses biometric values and self-selected authentication values as input data. Throughout recognition, it uses a cryptographically key and self-selected authentication values to acknowledge biometric values at intervals a gaggle error vary. What's additional, this methodology can use crypto graphical keys and input biometric values (within a planned error range) to revive the primary biometric values. [4] Vietnamese unit et al. projected associate application combining iris recognition and cryptography. the thought for this method is analogous to it of the fuzzy extractor in this they every use an error management code to simply settle for biometric values at intervals a ramification of errors. [5] John Daugman bestowed a fresh methods in Iris Recognition they were deals with the four advances in iris recognition: i) extra disciplined methods for detecting and dependably modelling the iris inner and outer boundaries with active contours, leading to extra versatile embedded coordinate system; ii) Fourier based mostly methods for determination problems in iris trig and projective geometry, allowing off-axis gaze to be handled by detecting it and "rotating" the eye into writing perspective; iii)applied science mutation methods for detecting and excluding eyelashes; iv) exploration of score normalizations, indulgent on the number of iris information that is offered in footage and thus the required scale of knowledge search. [6] Shanmugam Selvamuthukumaran, Shanmugasundaram Hariharan and Thirunavkarasu Ramkumar, bestowed a Investigation on iris recognition system.

A. Organization of paper

The paper is organized as follows; in section II we discuss about the problem definition of our work. In section III we discussed the related works of all the reference papers which we preferred. In section IV we describe the methodology from all the reference papers which we preferred. In section V we will discuss the conclusion of our work.

II. PROBLEM IDENTIFICATION

In largely papers and analysis that we've studied we have a tendency to see that the main downside that comes is the safety of the example options that are store within the info. Hackers will simply hack the example feature of the iris that's store into the info, as a result of in info the options are gift in their original type that's why they will simply get the first info. Therefore to beat from these issues we have a tendency to introduce a replacement technique that's nothing however the mixture of biometry and cryptography.

This paper presents a replacement secure authentication technique applying science techniques to biometric feature. The planned technique combines the benefits of biometric authentication and cryptography. By adding a system to existing biometric systems, the planned approach achieves the high security of cryptography techniques and therefore the tolerance for error of biometric recognition. This technique provides a high degree of security and is immune to power analysis attacks. as a result of the planned technique will be combined with science techniques, the identity verification may also apply cryptography techniques to make sure secure remote biometric matching.

III. RELATED WORKS

Shanmugam selvamuthukumaran, shanmugasundaram hariharan and thirunavkarasu ramkumar, conferred a paper or analysis work on Investigation on Iris Recognition System Adopting science Techniques. Throughout this paper they projected a method of optimized Iris Matching practice cyclic redundancy check. it had been together provides a distance calculation by CASIA. Throughout this the experimental data consisting of 900 iris footage in thirty classes were chosen and additionally the corresponding iris code is generated and keeps inside the data. The input image's code is compared with the whole opposite iris codes that unit of measurement keeps inside the data earlier [6]. Sr.Sagaya mother James provides a paper on "Iris recognition process". Throughout this paper she projected the strategy of iris recognition methodology, importance of binary conversion and therefore the means inner and outer sq. measures of iris area unit removed. She was primarily mentioned regarding the strategy of iris acquisition, iris localization, iris segmentation and together mentioned regarding the fringe detection (SCLERA-IRIS) and inner boundary detection (PUPIL-IRIS) [19]. Y.J.Chin, T.S.Ong, A.B.J.Teoh, K.O.M.Goh, presented a paper on integrated natural science example protection technique supported fingerprint & palm print feature level fusion. They propose to fuse multiple biometric modalities at the feature level therefore on get associate integrated example and to secure the united examples using a hybrid guide protection technique.

Their projected technique is made out of a feature transformation technique said as Random coating associated Associate in nursing equal-probable 2N discretization theme. Their experimental results show that the projected multi-biometric example protection theme demonstrates higher verification results as compared to their uni-biometric counterparts whereas protecting example security [9]. Sowmya.B, Sreedevi.S.L projected "Iris Recognition system for Biometric Identification". Throughout this paper, we tend to tend to propose associate economical technique for personal identification by analysing iris patterns that have a high level of stability and distinctiveness. With the increasing stress on security, automatic personal identification supported natural

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

science, has been receiving intensive attention over the past decade. The iris is, thanks to its distinctive biological properties, unit exceptionally fitted to identification. They jointly mentioned regarding the iris social control, iris segmentation, iris localization and have extraction and provide the biometric comparison of assorted technique [13].

"Identification of people by iris recognition" this paper was given by Gajendra singh chandel, Ankesh bhargava they projected the new technique of iris recognition "iris recognition by neural network". throughout this system initial collect the iris photos and pattern image method once this calculate the length of iris from right and high to bottom. Finally they use neural network for work and testing purpose. The recognition rate of this system was ninety seven.1%.this technique was less complicated the different technique [12]. John Daugman was provides a "New technique in Iris Recognition". This paper presents the following four advances in iris recognition: 1) extra disciplined ways that for police investigation and faithfully modelling the iris inner and outer boundaries with active contours, leading to extra versatile embedded coordinate systems;2) Fourier primarily based ways that for locating problems in iris trig and projective geometry, allowing off axis gaze to be handled by police investigation it and "rotating" the eye into writing perspective;3) applied mathematics thought ways that for police investigation and excluding eyelashes; and 4) exploration of score normalizations, looking forward to the amount of iris information that's out there in photos and additionally the required scale of knowledge search [5]. "An effective biometric crypto system combining finger prints with error correction codes" this systemgiven by the Peng Li, Xin Yang, Hua Qiao, Kai Cao, Eryun Liu, Jie Tian, Throughout paper, they projected a novel binary length-fixed feature generation technique of fingerprint. They together mentioned regarding the varied style of technique & offer together a comparison between those ways that.

IV. PROPOSED METHODOLOGY

The planned technique combines bioscience matching to appreciate crypto logical functions, like cryptography, authentication, identification, and key generation, which could be utilized in banks to exchange IC cards, seals, and various, suggests that of dual identification, thus guaranteeing privacy, integrity, no repudiation, so forth. These technologies area unit enforced through hardware or coding system applications and blend biometric systems in current use. Antecedent the man oeuvre was use for biometric identification wasn't able to provide complete security to carry on guide choices of the iris that unit gift inside the data. By applying this system, bioscience is combined with a crypto system thus enhancing the secure storage and use of biological feature data and effectively preventing malicious programs or attackers from stealing the biometric values or motility as legitimate users. This paper presents a secure cryptography-integrated biometric recognition technique with crypto logical functions. This system is prepared to integrate biometric matching with crypto logical technology to appreciate dual-factor authentication. This integrated technology can also be combined with additional advanced cryptanalytic techniques to provide safer and various applications.

The planned technique is split into a pair of components for description functions. The first [*fr1] is basic technique of improved iris recognition security (IRS) whereas the half is advanced technique of crypto logical technology. The agency technique is split into a pair of half: the registration part and so the matching section. The registration part initial provides a bunch of assorted iris connected data. Supported the varied choices of the iris, we have a tendency to tend to stipulate several numerical ranges, each of that comes with a quantization value. If the iris connected data fall at intervals one of these numerical ranges, then quantity the quantity the number} value for that numerical vary is utilized as a amount feature data to exchange the iris feature data. Next, unofficial operate operations unit accustomed convert the number feature data to hashed feature data.

Then, the excellence between the number feature data and so the iris image data is calculated to induce Associate in nursing adjustment value. Finally, this adjustment value is hold on with the hashed feature data. Matching and registration unit are largely similar. Initial we provide a registered hashed feature data and adjustment value, and so the biometric data then captured. The biometric data is adjusted supported this adjustment value. Next, (similarly) supported the varied choices of the iris, multiple numerical ranges unit printed, each of that will be a quantity value. If the adjusted biometric data fall at intervals one of the numerical ranges, then the number value of this value vary is taken as a result of the number feature to exchange the adjusted biometric data. This could be followed by unofficial operate operations to convert the number feature into hashed feature data. Finally, the registered hashed data is compared with the hashed feature data. Inside the advance cryptography technology technique, the biometric data ought to initial endure iris recognition security technique before it's utilized during this technique. This technique integrates the cryptography technology for iris recognition application pattern the biometric data that consists of the "registration" and "verification" stages. The appliance provides biometric-based crypto logical field for the friend.

A. Cryptography technique:

The word cryptography today refers to the science and the art of transforming message to make them secure and immune to attack, the original message before transferred called plain text, after message is transform it is called cipher text. The sender use encryption technique and the receiver use decryption technique. There are some component of the cryptography that helps hiding the information. In the cryptography technique key is the most important parameter of this technique. Key is a value or a number the cipher is an algorithm operates on the key for the encryption of a message. We have to use an encryption algorithm and encryption key and the plain text at the input. At the output of encryption we get the cipher text for decryption of cipher text. We have to use decryption

algorithm a decryption key and the cipher text at the input after we get the plain text back. Thus our proposed methodology is used this technique for hiding the original iris feature template.

Flow chart of this iris recognition technique by using cryptosystem is shown below. This flow chart are consist of two part first is registration phase and second is authentication phase.

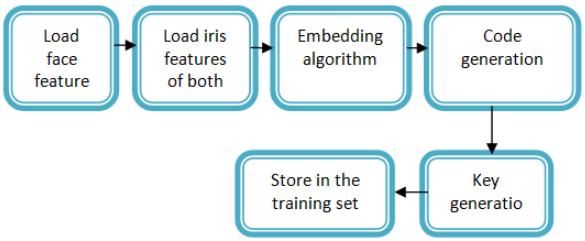

Fig.1- Registration phase of iris image

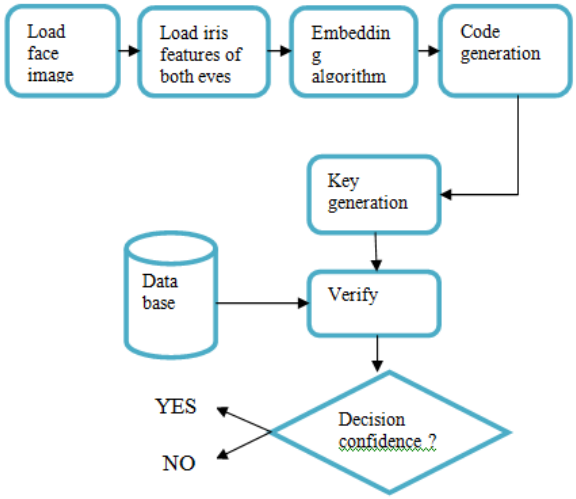

Fig .2-Authentication phase of iris image

V. CONCLUSION

Iris recognition technology provides uneven accuracy and speed. During this paper, associate in Nursing economical technique for private identification and verification with iris patterns are bestowed. We might be making an attempt to make a secure intense project within which security would a significant issue, so creating security with the extraordinary algorithmic program of cryptography and adding biometric identification to that. Numerous approaches adopted by researchers to secure the raw biometric knowledge and model in knowledge base a mentioned here. During this paper a way is projected to store iris model firmly within the info victimization cryptography algorithmic program. The benefits of such style of cryptanalytic them are original image security is provided secure authentication. Likelihood to faux share creation isn't attainable, over one image be unbroken as secret. Coding and secret writing technique of cryptography is initially of the ideas to be enforced for security.

ACKNOWLEDGMENT

We express our thanks to **Mr. R. M. Potdar,** Sr. Associate Professor, Dept. of ETC, BIT Durg and acknowledge the timely help of **Dr. T. Siva Kumar,** Sr. Associate Professor, Dept. of ETC, BIT Durg. We warmly thank **Dr. Manisha Sharma,** HOD Dept. of ETC, BIT Durg for her kind support and guidance.

Above all we render our gratitude to all those who wished us success.

REFERENCES

[1]. Lakshmi madhuri.k, Viraj thakur, Rajesh jaiswal, Sandesh sonawane, Rohit nalavade "biometric data security using recursive visual cryptography" Information and knowledge Management ISSN 2224-5758, Vol. 2, 2012.
[2]. CAI li, Jiankun hu, Josef pieprzyk, Willy susilo, "A New Bio-cryptosystem-oriented security analysis framework and implementation of multi-biometric cryptosystems based on decision level fusion" IEEE Transactions on Information Forensics and Security, 2015.
[3]. Dodis Y, Reyzin L, Smith A. Fuzzy extractors: how to generate strong keys from biometrics and other noisy data. Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT '04); May 2004; Interlaken, Switzerland.
[4]. Hao F, Anderson R, Daugman J. UCAMCL-TR-640. Cambridge, UK: University of Cambridge, Computer Laboratory; 2005. Combining cryptography with biometrics effectively.
[5]. John Daugman, "New Methods in Iris Recognition" IEEE TRANSACTION ON SYSTEM, MAN, AND CYBERNETICS-PART B: CYBERNETICS, VOL.37, NO.5, and OCTOBER 2007.
[6]. Shanmugam Selvamuthukumaran, Shanmugasundaram Hariharan and Thirunavkarasu Ramkumar, "Investigation on Iris Recognition System Adopting Cryptographic Technique" The International Arab Journal of Information Technology, Vol. 12, No.1, January 2015.
[7]. Mayank vats, Richa singh, Afzel noore, "Improving iris recognition performance using segmentation, quality enhancement , match score fusion , and indexing" IEEE TRANSACTION ON SYSTEMS, MAN AND CYBERNETICS-PART B: CYBERNETICS, 2008.
[8]. Peng Li, Xin Yang, Hua Qiao, Kai Cao, Eryun Liu, Jie Tian "An effective biometrics cryptosystem combining fingerprints with error correction codes", Expert system with application 39 (6562-6579) ,2012.
[9]. Y.J.Chin, T.S.Ong, A.B.J.Teoh, K.O.M.Goh, "Integrated biometrics template protection technique based on fingerprint & palm print feature level fusion", Information fusion 18 (161-174) 2014.
[10]. Surbhi garg, Harmeet kaur, "Survey paper on phase based iris recognition" International journal of advanced research in computer science and software engineering, volume 4, April 2014.
[11]. Shweta arora, Narendra D. Londhe, Anuja kumar acharya, "Human identification based on iris recognition for distant images", International journal of computer applications (0975-8887) Vol. 45-no.16, may 2012.
[12]. Gajendra singh chandel, Ankesh bhargava, "Identification of people by iris recognition" International journal of computer science and network security, vol.14 no.3, march 2014.
[13]. Sowmya.B, Sreedevi.S.L "Iris recognition system for biometric identification", International Journal of emerging trends & technology in Computer science (2278-6856) may 2013.
[14]. Tajinder pal singh and Sheifaligupta, "Enhancing performance of iris recognition algorithm through time reduction", International journal of signal processing, image processing and pattern recognition, vol.7.no.4, pp.57-64, 2014.
[15]. J. Daugman, United States Patent No. 5,291,560. Biometric Personal Identification System Based on Iris Analysis, Washington DC: U.S. Government Printing Office, 1994.
[16]. J. Daugman, "The Importance of Being Random: Statistical Principles of Iris Recognition," Pattern Recognition, vol. 36, no. 2, pp 279-291.

[17]. J.Daugman, "How iris recognition works", IEEE Transaction on circuit and system for video technology, vol.14, no. 01, January, 2004.
[18]. F.Hao, J.Daugman and P.Zielinski, "A fast search algorithm for a large fuzzy database", IEEE Trans .Inf.Forensic Security, Vol.3, no.2, JUNE, 2008.
[19]. Sr.Sagaya Mary James, "Iris recognition process", proceedings of the UGC sponsored national conference on advanced networking and applications, March, 2015.
[20]. Uludag, U., Pankanti, S., Prabhakar, S., & Jain, A. (2004). Biometric cryptosystems: Issues and challenges. Proceedings of the IEEE, 92(6), 948–960.

BIOGRAPHY

Pooja, she is received the B.E degree in Electronics and Tele communication engineering from Bhilai Institute of Technology, Raipur (India) in 2014, currently pursuing ME degree in electronics and telecommunication engineering at Bhilai Institute of Technology, Durg (India). Pooja has field of interest is image processing.

DOI 10.17148/IJARCCE.2016.5386