IJCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.-7, Special Issue, 6, March 2019 E-ISSN: 2347-2693

Analysis on Biometrics, Forensics Protecting Using Key Binding Mode Based Ppbss Using Fuzzy Vault

Syed Javid Basha [1*], B. Muni Hema Kumar[2]

[1,2]Dept. of MCA, Srikalahastiswara Institute of Information and Management Sciences, S.V.University, Tirupati, India

Corresponding Author: javidbasha05@gmail.com

DOI: https://doi.org/10.26438/ijcse/v7si6.116121 | Available online at: www.ijcseonline.org

***Abstract*—** Direct storage of biometric templates in databases exposes the authentication system and legitimate users to numerous security and privacy challenges. Human beings can no longer be separated from electronic devices and the Internet technology. The need for information made available on systems and networks which are connected on the internet. It is very essential to provide an effective security measure and system that ensures the confidentiality, integrity, and availability of information system, networks, and the services and resources made available. In this paper a new way of technique is Fuzzy vault. Fuzzy Vault is one of the most promising bio-cryptographic techniques to prevent the template data from being misused. To make the fuzzy vault practically realizable in real-life applications especially for large databases, the chaff generation time needs to be reduced to greater extent. This work focuses on decreasing the chaff generation time to reduce the overall vault creation time This can be achieved using Biometric and Digital Forensic Technology.

***Keywords*—** Biometrics, Digital Forensic Technology, Biometric Security, fingerprint recognition, Fuzzy Vault, Chaff Points.

I. Introduction

Security is currently a widespread and growing concern that affects all aspect of society: business, domestic, financial, government, and so on. The information society is increasingly dependent on a wide range of networks and systems whose mission is critical, such as air traffic control systems, financial systems, or public health systems [1]. Information is a critical asset of every organization due to their rapid adoption of IT (Information Technologies) into their overall business activities. This has increased the need for an effective management of the companies and institutions information. Currently, information is an asset that is as important as a company or institution's capital or work. In fact, this has born the reality of the need for information security and network management. In new generation companies and institutions, this reality is even more pressing because information one of their core business. Thus, the dependence on Information Systems (IS), and networks has skyrocketed in the last few years, hence there is need to effectively protect the information that is transmitted across these systems and networks in other to maximize their potentials [2].

Further-more, because of the exponential growth of the Internet, identity verification becomes an essential part in web-based applications, such as online banking and online shopping. A pin number can be shared by many people and an identity card can be stolen by someone. Moreover, attackers can get access to a system by guessing passwords and pin numbers.

In order to overcome the issues the traditional verification methods, human biological characteristics have been exploited to develop biometric based verification systems. Biometric verification is defined as the verification of an individual based on the physical, chemical or behavioral attributes of the person [2]. The main advantage of using biometric traits is identity verification a system is that they cannot be easily shared or stolen. In addition to this, biometric schemes are easier to use, as users do not need to remember passwords, pin numbers or carry their identification cards.

Although the biometric based verification systems have obvious advantages over the traditional ones, such systems can risk the privacy of individuals if they are not designed appropriately. For example, a biometric system may store fingerprints or iris data. If the biometric data is exposed to an attacker, the latter can be used for undesired purposes such as impersonation. More importantly, since the biometric data is derived from the biological characteristics of individuals, they cannot be altered. Thus, the leakage of the biometric data can cause serious and continuous threats to the privacy of individuals. Therefore, the biometric data should be protected in such a way that even if it is compromised, the attacker still cannot gather any information which can breach individuals' privacy. Besides, an attacker should not be able to login as a genuine user[3].

Biometrics: A Strong Alternative for Crime Detection

Biometric technology makes a contribution to crime detection by associating the traces to the persons stored in the database, ranking the identity of persons and selecting subdivision of persons from which the trace may originate.

A biometric system is a pattern recognition device that acquires physical or behavioral data from an individual, extracts a salient feature set from the data, compares this features set against the features set stored in the database and provides the result of the comparison. Therefore, a biometric system is composed of four modules [2].

Sensor Module: This component acquires the raw biometric data of an individual by scanning and reading. For example, in case of fingerprint recognition, an optical fingerprint sensor may be used to image the ridge pattern of the fingertip. The quality of raw data is influenced by the scanning or camera device that is used.

Quality assessment and features extraction module: For further processing, the quality of the acquired raw data is first accessed. The raw data is subjected to signal enhancement algorithm to improve its quality. This data is then processed and a set of salient features extracted to represent the underlying trait. This feature set is stored in the database and is referred as a template. For example, the position and orientation of minutia in a finger print image is extracted by the feature extracted by the feature extraction module in finger print biometric system.

Matching and decision making module: In this module, the extracted templates are then matched against the stored templates and a matching score is given. On the basis of the matching score, the identity of a person is validated or ranked.

System database module: This module acts as storage of biometric system. During the enrollment process, the template extracted from raw biometric data is stored in the database along with some biographic information (such as name, address, etc.) of the user.
en we look all the roles performed by an attacker on IoT.

II. RELATED WORK

Digital forensics is defined as a scientifically proven method for the investigation of computers and other digital devices suspected to be involved in criminal activities and network attacks [4]. It was innovated as an avenue to suppress the increase of computer and network attacks. Proper digital forensic procedures and process model should be followed for its evidences to be admissible in a court of law for prosecution of offenders. Digital forensics applications cover several aspects which includes; the need for the law of enforcement to produce the compelling and legally accepted evidences required for crime prosecution, the need for institutions and cooperation to identify and mitigate insider threats [5]. Tools for computer forensics is used to collect, analyze and extract evidence after intrusions. Demand for forensics techniques examination is already much greater than current capacity. Therefore, this research proposes digital forensic and biometric analysis for information security and network management. It aims at establishing that biometric feature authentication guarantees accurate user identification, and also enables digital forensic investigation should there be any security violation and attack. It provides legal evidences which are admissible in court for prosecution of offenders and attackers. However, combating these attacks that replicate on daily basis has become a major global concern. Apparently, the research idea majorly on how to better identify users or parties to enable forensic investigators such that culprits(attackers and intruders) are identified and prosecuted in other to pay their due to penalties. This research therefore, proposed Digital Forensics and Biometric Analysis (DFBA) for information systems and network security. It specifies the significance of biometric features such as face recognition and finger prints in forensic investigation. Also, it emphasizes that the use of biometric authentication will enable forensic finding and investigations [6].

Biometric and Digital Forensic Analysis Architecture:-

This section focuses on the requirement analysis and design of biometric and digital forensic analysis architecture. It also specifies the different stages and phases that makeup the BDFA architecture. The BDFA architecture is introduced to provide a response to the problem statement and the main objective of this research paper.

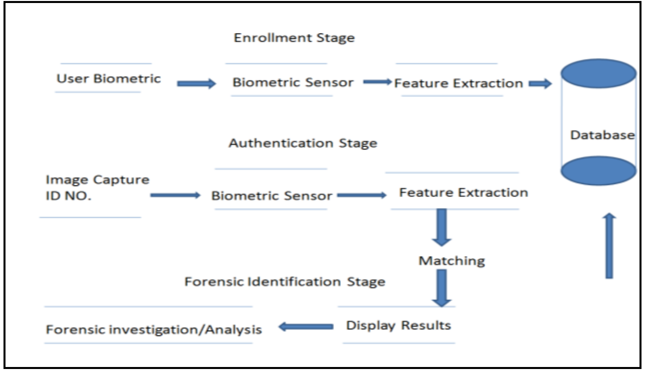


Figure 1: Biometric and Digital Forensic Analysis Architecture

However, the BDFA system architecture is used to describe the overall design, structure and behaviour of the system. It provides formal description and representation of the system in a way that supports the exact concept of the paper.

III. METHODOLOGY

Digital forensics and biometric are tightly coupled. Forensic information can be available from biometric systems. This research intends to establish a link between digital forensic(DF) and biometric technology (BT). Also, establish a possibility of biometric based authentication enabling digital forensic investigation. It establishes that biometric features to provide a better access control , identification and authentication of any given party which helps in forensic investigation involves a group of defined procedures and task for experimental purpose. This procedures and tasks are used to extract useful information from digital devices shown in fig 1 as evidences to commence legal proceedings in court. However, the procedures includes: preparation, data collection, examination data analysis, and reporting or presentation of findings. Preparation and data collection is the first phase in the process which is primarily to identify, label, record, and acquire relevant data from all possible sources of information.

The second phase is examinations which involve forensically processing large amount of collected data using a combination of automated and manual methods to assess and extract data of particular interest. The next phase of the process is analysis which is to analyze the result of the examination, using legally justifiable methods and techniques, to derive useful information that addresses the questions that constitutes the reason for conducting the data collection and Examination. Lastly, is reporting the results of the analysis, or the presentation of findings which may include describing the actions used, explaining how tools and procedures were selected, determining what other actions need to be performed, and providing recommendations for improvement to policies, guidelines, procedures, tools, and other actions need to be performed, and providing recommendations for improvement to policies, guidelines , procedures, tools, and other aspects of the forensic process[6].

However , analysis(data analysis) is one of the complex stages in digital forensic investigation. The analysis stage of forensic investigation involves; data analysis, survey, extraction and examination. Digital forensic as defined by the digital forensic research workshop (DFRWS) is the use of scientifically derived and proven methods towards the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal or helping to anticipate unauthorized actions shown to be disruptive to planned operations.

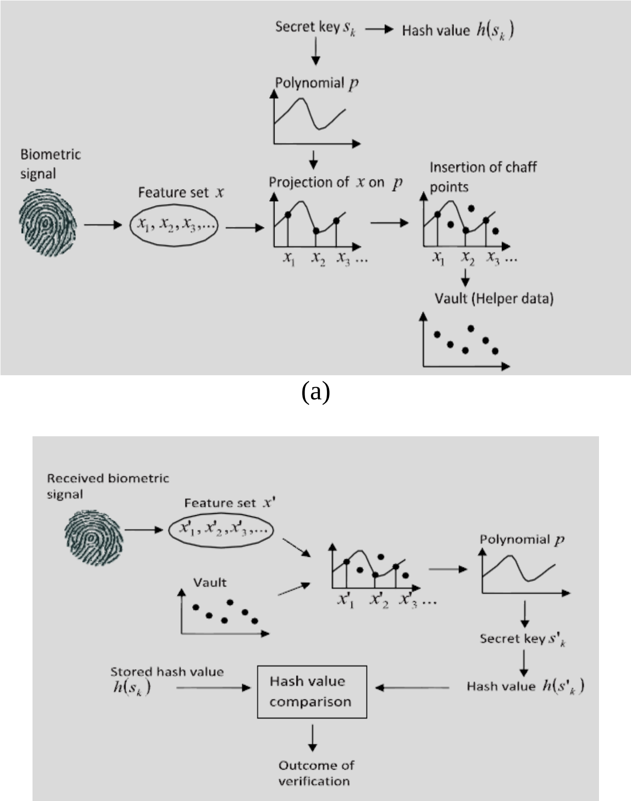
This definition embraces the broad aspects of digital forensic from data acquisition to legal actions. Analysis begins after data has been acquired or collected from the suspected system or crime scene. It basically involves critical extermination of the acquired data in other to identify evidence. Therefore, digital forensic analysis can be referred to as identifying digital evidence scientifically derived with proven methods that can be used to facilitate or further the reconstruction of events in an investigation [6]. Obviously, like any other investigation of events, to find the truth data must be identified in other to either verify existing data and theories or to contradict existing data and theories. Before both evidences can be extracted from a collected data, it must be thoroughly analyzed and identified.

The task or challenge of digital forensic analysis is to identify the necessary evidence for legal proceedings in court[6]. On the other side , biometric identify based verification technology offers more reliable individual identification which support digital forensic investigation. One of the questions this research tends to address is, how can biometric technology (BT) help DF perspective? It analyses a biometric situation while justifying the research objectives by providing answers to the research questions.

Key Binding Mode Based PPBSs Using Fuzzy Vault: Fuzzy vault is a popular error resistant technique initially proposed by Jules and Sudan [7]. It is designed to work with unordered sets (Ex. Important feature points, known as minutiae points, in fingerprints) and has the ability to deal with interclass variations which is commonly encountered in biometric data Fig 2 illustrates the basic key binding mode based PPBS using fuzzy vault. First of all, from the biometric signal such as a fingerprint, a biometric feature set x is extracted. Besides, based on the secret key s_k, , a corresponding polynomial p is generated e.g., the elements of s_k could be used to for the coefficients of p. Then, the projection of the unordered biometric feature set x on the polynomial p is calculated.

After that, the random points which do not lie on the polynomial p, called chaff points, are added to the calculated projected points. Denote both sets of points (i.e.., the projected points on the polynomial and the added chaff points) as v. In a PPBS using fuzzy vault, the helper data v is popularly known as the vault. Here, the chaff points are added to conceal the polynomial p from an attacker. In addition to v, the hash value of the secret key, denoted as $h(s_k)$, is also stored during the enrolment process. At the verification stage, to successfully unlock the vault v, a set of biometric features x’ is needed. If the received biometric feature set x’ largely overlaps with x, one can locate adequate number of points in v, which lie on the polynomial p. From p, the secret key s'_k can be extracted. Finally, verification is done by comparing the hash value of the derived secret key, $h(s'_k)$, and the stored $h(s'_k)$.

The first working key binding mode based PPBS using fuzzy vault was introduced by Clancy et al [8], where the pre-aligned feature set from fingerprints was assumed. Due to this assumption, the practicality of this method is very limited. To remove this assumption, Nandakumar et al. introduced a method utilizing the high curvature points derived from the orientation field of fingerprints [9]. Differently to overcome the alignment issue, Li et al. proposed to fuse the local features and local structures to withstand geometric transformation such as rotation and translation [10]. In [11], the orientation information of the biometric data was employed to increase verification accuracy. While verification accuracy can also be improved by increasing the number of chaff points, the increase of chaff points will inevitably raise computational complexity. In [11], Nguyen et al. proposed a mechanism to generate chaff points in a faster and more efficient way. It is worth mentioning that although the PPBSs using fuzzy vault where initially applied to fingerprints, they are also applicable to other biometric signals such as iris [12], palm prints [13], and face biometric [14].



(a)

(b)

Figure 2. Illustration of basic key binding mode based PPBS using fuzzy vault (a) Enrolment; (b) Verification

IV. ALGORITHMS USED

Proposed Chaff Generation Methodology –

The proposed chaff generation approach modifies the chaff generation process for the base algorithms of Clancy et al. [15] and Nguyen et al.[16],[17]. Both the algorithms compute Euclidean distance for the distance comparisons between the selected point and a genuine minutiae point. However, the Euclidean distance computations are complex and more time consuming as they require the square and square root computations. The proposed approach makes use of Manhattan distance instead of Euclidean distance, which leads to significant reduction in the chaff generation time. The modified approach is less compute intensive as it eliminates the need for complex square and square root operations. The approach work as well as the absolute distance comparisons are not required for classifying any candidate chaff point as a valid chaff point and for this purpose only relative distance comparisons may work based upon an optimized threshold value. The equivalence established between Euclidean distance and Manhattan distance and $\Delta x=(x-x_1)$ and $\Delta y=(y-y1)$ for two points (x, y) and (x1,y1),

$$D_{(Eucl)=}\sqrt{(\Delta x)^2{}_{+}(\Delta y)^2} \tag{1}$$

$$D_{(Man)}=(|\Delta x| + |\Delta y|) \tag{2}$$

$$(\Delta x)^2 + (\Delta y)^2 = (\Delta x)^2 + (\Delta y)^2$$

Add 2 $|\Delta x \, \Delta y|$ to R.H.S.

$$(\Delta x)^2+(\Delta y)^2 \le (\Delta x)^2+2|\Delta x \, \Delta y|+(\Delta y)^2$$

So,

$$(\Delta x)^2+(\Delta y)^2 \le (|\Delta x| + |\Delta y|)^2 \tag{3}$$

From (1) , (2), and (3)

$$(D_{(Eucl)}))^2 \le (D_{(Man)})^2 \tag{4}$$

since the square of a real number is non-negative

$$(\Delta x)^2-2|\Delta x \, \Delta y|+(\Delta y)^2=(|\Delta x| - |\Delta y|)^2 \ge 0 \tag{5}$$

Add$(|\Delta x| + |\Delta y|)^2$ to both sides

$$(|\Delta x| - |\Delta y|)^2+(|\Delta x| + |\Delta y|)^2 \ge (|\Delta x| + |\Delta y|)^2 \tag{6}$$

$$(\Delta x)^2- 2|\Delta x \, \Delta y|+(\Delta y)^2+(\Delta x)^2+2|\Delta x \, \Delta y|+(\Delta y)^2 \ge (|\Delta x| + |\Delta y|)^2$$

$$2\times ((\Delta x)^2 +(\Delta y)^2) \ge (|\Delta x| + |\Delta y|)^2 \tag{7}$$

From (5), (6), and (7)

$$2\times(D_{(Eucl)})^2 \ge (D_{(Man)})^2 \tag{8}$$

From (7) and (8) it can be conclude that

$$D_{(Man)}= f (D_{(Eucl)})$$

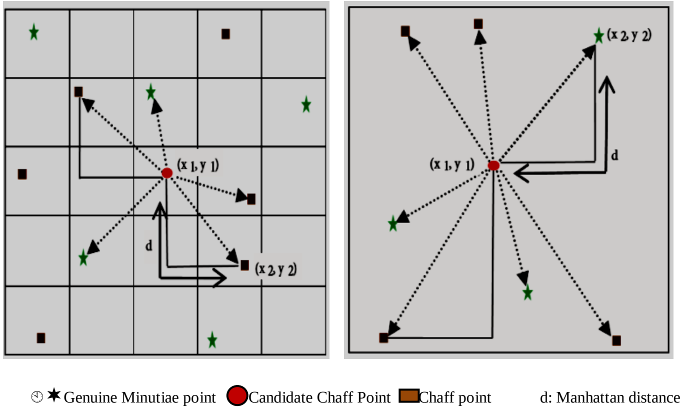
$$(D_{(Eucl)})^2 \le (D_{(Man)})^2 \ \&\& \ 2\times(D_{(Eucl)})^2 \ge (D_{(Man)})^2 \tag{9}$$

Now assuming $\delta_{(Eucl)}$ as a threshold value in Euclidean distance and $\delta_{(Man)}$ as a threshold in Manhattan distance, the relation between the two threshold values can be established from (9) as

$$(\delta_{(Eucl)})^2 \le (\delta_{(Man)})^2 \ \&\& \ 2 \times (\delta_{(Eucl)})^2 \ge (\delta_{(Man)})^2 \tag{10}$$

Thus the condition specifies limits (maxima and minima) on the value of δ and the floor value of average of these maxima and minima may be taken as $\delta_{(Man)}$.

Steps of the proposed approach are as follows:
Step 1: Acquire the fingerprint image.
Step 2:Apply the pre-processing steps as binarization, thresholding , thinning etc. on it.
Step 3: Apply crossing number approach [1,9] to extract genuine minutiae point as
GM={m1,m2…mj} where mj represent the coordinates(x,y) for a minutiae point.
Step 4: To add chaff points in genuine Minutiae set GM, Clancy's [15] and Nguyen's[16,17] approaches of chaff point addition are modified as illustrated in Figure 3 and discussed below in Sections 3.1 and 3.2, respectively.



(a)Clancy's Approach *(b) Modified Nguyen's Approach*

Figure 3: Illustration of Modified Approach

Modified Clancy's Approach –

Clancy modified original fuzzy vault as proposed by Jules and Sudan[15], with the justification that the chaff points/random points to be added to the set of genuine points to form a vault should be placed at an appropriate distance 'd' apart from vault members.

It makes use of Euclidian distance as a metric for comparing the distance between the new chaff point o be added with the existing list of points (genuine minutiae points and chaff points), which makes the approach more compute intensive. To improve upon it, the proposed modifications in the existing approach as below:

i. Consider a vault list (VL) = GM
ii. Generate a random point (x, y) in the image. To qualify the chosen point as a chaff point it has to be δ distance apart from all the points in VL. Value of δ in the case o the modified Clancy's approach is computed using Eq(10).
iii. Compute the Manhattan distance'd' between the selected point (x1, y1) and other existing points (x_i, y_i) in the vault list.

$$d= |x-x_i| + |y-y_i|$$

iv. If d ≥ δ(Man) for all points in VL
Then (x, y) qualifies as chaff point and add (x, y) to VL
else
generate new random point.
v. Repeat the steps ii, iii, iv to generate the required number of chaff points.

Modified Nguyen's approach:-

Nguyen's approach gave significant time reduction compared with Clancy [15] and Khalil-Hani [18], especially when the number if minutiae points is above 20. However, this approach still makes use of Euclidean distance as a measure. The steps to be followed in the modified approach are described below:

i. Consider a vault list(VL) = GM
ii. Split fingerprint image into equispaced cells of square matrix.
iii. Choose a random cell.
iv. If (random cell contains a genuine minutiae point or chaff point)
Discard it and go to step iii
Else
Consider the cell for candidate chaff point and select a random point(x_1, y_1)
v. Compute Manhattan distance 'd' among (x_1, y_1) and points in its eight adjacent neighborhood cells ($N_8(p)$) from the VL.
vi. Using Eq.(10) $\delta_{(Man)}$, a threshold value is computed for modified Nguyen's approach
vii. If ≥ $\delta_{(Man)}$ for all $N_8(P)$ (eight adjacent pixels), where p is (x_1, y_1) then qualifies as a chaff point and add (x_1, y_1) to VL
Then (x_1, y_1) qualifies as a chaff point and add (x_1,y_1) to VL
else
discard (x_1, y_1) as chaff point
viii. Repeat the steps from iii to vii to generate the required number of chaff points.

The proposed approach works well as by using Manhattan distance instead of Euclidean distance the chaff generation time is reduced significantly especially in worst case comparisons when for each chaff point addition the distance of all eight adjacent cells from the candidate cell needs to be compared. The modified approach is less compute intensive as it eliminates the need for complex square and square root operations. The approach works well as the absolute distance comparisons are not required and only relative distance comparisons may work and the value δ (threshold) is adjusted as per Eq.(10).

V. CONCLUSION AND FUTURE SCOPE

It has been observed in the experimental results that the time required for chaff generation is reduced to a greater extent in the case of modified Clancy's and modified Nguyen's approaches by using the Manhattan distance as a metric of distance comparison while generating a new chaff point. The approach also reduces the complex computations to simple one. Since the proposed approach has been evaluated on dedicated hardware, it can be deployed in real-time application scenarios.

REFERENCES

[1] Fish JT, Miller LS, Braswell MC (2013) Crime scene investigation Routledge.

[2] A.K Jain, P. Flynn, and A.A Ross, Handbook of Biometrics, New York, NY, USA: Spinter, 2008

[3] A. Cavoukian and A. Stoianov, "Biometric encryption," Encyclopedia of Cryptography and Security, New York, NY, USA: Springer, 2009.

[4] Opdahl, A. L. and G. Sindre "Experimental comparison of attack trees and misuse cases for security threat identification."Information and software Technology. In press, Corrected proof, 2008.

[5] N.S.Sargur, C.Huang, S. Harish, V. Shah. "Biometric and Forensic aspects of Digital Document Processing," 2010, PP.720-728.

[6]G. Pangalos, C. Linoudis,and I. pagkalos." The Importance of Cooperate Forensic Readlines in the information Security Framework," in *proceedings of IEEE Workshop on Enabling Technologies infrastructure for collaborative Enterprise "* 2010, PP.12-18

[7] A.Juels and M.Sudan "A Fuzzy valut scheme", in Proc IEEE int. Symp. Inf, Theory, Jul 2002, p. 408

[8] T.C Clancy, N Kiyavash, and D.L Lin, "Secure Smartcard based fingerprint authentication, " in Proc. ACM SIGMM workshop Biometrics Methods Appl 2003, pp 45-52.

[9] K. Nandakumar, A.K Jain, and S.Pankanti, "Fingerprint – based fuzzy vault: implementation and performance," IEEE Trans, Inf. Forensics, Security, vol 2, no 4, pp 744 – 757, Dec 2007.

[10] P. Li X Yang, K Cao , X Tao, R.Wang, and J Tian, "An alignment – free fingerprint cryptosystem based onfuzzy vault schemen,: J. Netw, Comput. Appl., vol 33, pp 207-220, 2010.

[11] A.Nagar, K. Nandakumar, A.K Jain, and S.Pankanti, "Fingerprint – based fuzzy vault: implementation and performance," IEEE Trans, Inf. Forensics, Security, vol 2, no 4, pp 744 – 757, Dec 2008.

[12]T.H Nguyen, Y.Wang, Y.Ha, and RLi " Improved chaff point generation for vault scheme in bio-cryptosystems," IET Biometrics, vol 2, no2 pp 48-55, Jun 2013.

[13]X.Wu, N.Qi, K. Wang, and D Zhang, "A novel cryptosystem base on iris key generation," in Proc 4th Int. conf. Natural comput. 2008, pp 53-56.

[14]Y.Wu and B. Qiu, "Transforming a pattern identifier into biometric key generators," in Proc. IEEE int Conf. Multimedia Expo, Jul 2010 pp 78-82.

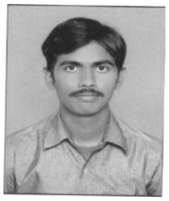
[15]Clancy TC, Kiyavash N, Lin Dj Secure smart-card based finger print authentication. In: proceedings of the 2003.

[16] Nguyen TH, Wang Y, Nguyen TN, Li R, A fingerprint fuzzy valut scheme using a fast chaff point generation algorithm. IEEE 2013 International conference on Signal Processing, Communication and Computing; 5-8 August 2013

[17] Nguyen TH, Wang Y, Nguyen TN, Li R, Improved chaff point generation for vault scheme in bio-cryptosystems. IET Biometrices 2013; 2: 48-55

[18] Benhammadi F, Bey KB Password hardened fuzzy vault for fingerprint authentication system. Image vision comput 2014; 32: 487-496

Authors Profile



Mr. Syed Javid Basha, Student received his Graduate Degree in B.Sc. Computer Science from Sri Venkateswara University, Tirupathi in the year of 2013-2016. Pursuing Master of Computer Applications from Sri Kalahastiswara Institute of Information and Management Sciences, Sri Kalahasti, Affiliated to Sri Venkateswara University, Tirupathi in the year 2016-2019. His research interests include Data Communication and Computer Networks.

B. MUNI HEMA KUMAR received his Graduate Degree in B.Sc. Computer Science from Sri Venkateswara University, Tirupathi, in the year of 2003-2006. He received his Master of Computer Science (MSc-Cs) Degree from Sri Venkateswara University, Tirupathi, in the year 2006-2008. He has over 8 Years of teaching experience in the area of computer Science and he has published papers at various International Conferences and Journals. His research interests include Java, Computer Organization, Data Structures, Cobol, Computer Networks and Web Programming. Currently, he has been working as an Assistant Professor in the Department of MCA from Sri Kalahastiswara Institute of Information and Management Sciences, Srikalahasti.