Biometric Security Systems and Contemporary Affirmation of State of Art

P.Srinivas[1] **D r.P.V.S.Srinivas**[2]

[1] **Associate Professor, CSE Department, Geethanjali College of Engineering & Technology, Hyderabad, A.P, India.**
Email id: pattlolasrinivas@gmail.com
[2] **Professor & Head, CSE Department, Geethanjali College of Engineering & Technology, Hyderabad, A.P, India.**

Abstract: Biometrics is playing vital role in applications that are centric to tasks such as identification, verification and classification. One distinctive illustration is a biometric verification structure that concludes the user's authorization by validating the biometric traits submitted by the user. The human traits preferred for biometric systems are universally unique and stable for long time. Moreover the biometrics based verification structures are free from hassles such as opting to complex passwords, remembering and protecting them. The human traits used for biometrics based authentication are user specific and available to others for unauthorized usage is impractical. Henceforth it is quite obvious to consider these biometrics based security structures are strong alternative to traditional password based authentication strategies or effective to progress the security standards of the traditional authentication models. Here in this research article we explore the taxonomy and contemporary affirmation of the biometrics under privacy and security concerns in recent literature.

Index terms: Biometric security, unimodal biometric systems, multimodal biometric systems, visual crypto biometric systems, Identity leakages, privacy leakages, feature Transformations, Biometric crypto Systems

1. INTRODUCTION:

Biometrics is defined as the exclusive (individual) physical/logical characteristics or behavior of human body [1]. These characteristics and behavior are used to recognize each human. Any particulars of the human body which diverges from one to other will be utilized as exclusive biometric data to provide as that individual's inimitable identification (ID), for instance retinal, iris, palm print, fingerprint, and DNA. Biometric structures will amass and lay up this data in order to employ it for confirming individual distinctiveness. The grouping of biometric data structures and biometrics authentication technologies produces the biometric security structures. The biometric security structures are a catch and confine mechanism to organize admission to particular data. In order to admittance the biometric security structure, an individual will need to provide their unique characteristics or behavior which will be matched to a database in the structure. If there is a match, the catch structure will afford access to the data for the user. The catching and confining structure will activate and record information of users who admittance the data. The association between the biometric and biometric security structure is also known as the lock and key structure. The biometrics security structure is the lock and biometrics is the key to open that lock [2]. A set of criteria are exists for biometric security structure, which are exclusivity, generality, stability, bring together, performance, adequacy and circumvention [3]. As mentioned above, uniqueness is considered as the priority one requirement for biometric data. It will designate how another way and exclusively the biometric structure will be able to recognize each user among groups of users. For case in point, the DNA of each individual is unique and it is impossible to replicate.

Universality is the inferior criterion for the biometric security. This parameter designates necessities for distinctive characteristics of each individual in the world, which cannot be simulated. For example, retinal and iris are characteristics will convince this stipulation. Thirdly, a solidity parameter is requisite for every single characteristic or trait which is recorded in the database of the structure and needs to be constant for a certain period of time period. This parameter will frequently be exaggerated by the age of the user. Following the durability parameter is the collective. The collective parameter entails the collection of apiece characteristic and attribute by the structure in order to validate their credentials. Then, performance is the subsequent parameter for the structure which outlines how well the security structure works. The correctness and heftiness are major issues for the biometric security structure. These issues will settle on the performance of the biometric security structure. The suitability stricture will decide fields in which biometric technologies are tolerable. Finally, circumvention will settle on how easily each characteristic and characteristic provided by the user can direct to failure through the confirmation process. DNA is whispered to be the most convoluted characteristic leading to the failure of the authentication process [4].

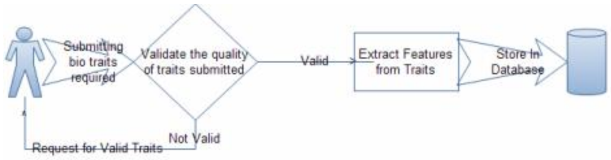
2. NOMENCLATURE OF THE BIOMETRIC SYSTEMS

2.1 Measurement requirements

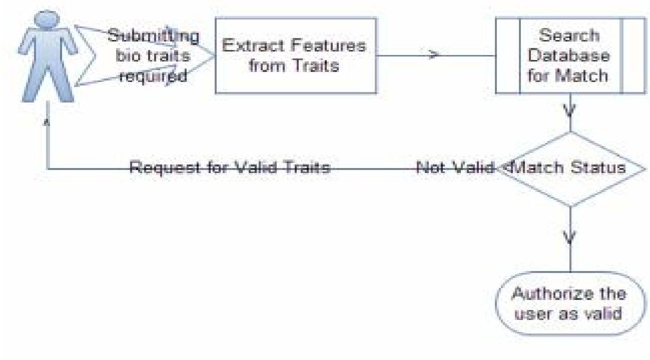
The needs to be satisfied by the characteristics related to physiology or manners of a human to consider as parameters for biometric system (1) Generality (the features related to Physiology or behavior should reflect) (2) Distinctiveness (divergence in these features regard to any two individuals is must), (3) Durability (the features should be adequately similar over a period of time) and (4) Collectiveness (the features should be feasible to apply quantitative measurement models).

The other factors such as performance, adequate, exactness, pace, resource necessities and dodging should take into account for best practical usage of biometric systems. In other words, a practical system must be undisruptive, received by the projected users, and suitably tough to a variety of falsified methods and attacks.

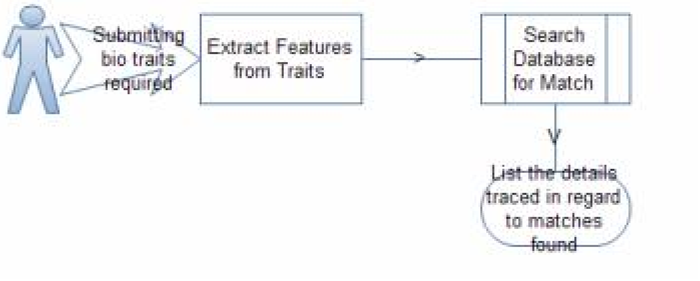
2.2 Biometric systems


Submitting bio traits required
Validate the quality of traits submitted
Valid
Extract Features from Traits
Store in Database
Not Valid
Request for Valid Traits

Registration process of an individual


Submitting bio traits required
Extract Features from Traits
Search Database for Match
Request for Valid Traits
Not Valid
Match Status
Authorize the user as valid

Authentication Process of an individual


Submitting bio traits required
Extract Features from Traits
Search Database for Match
List the details traced in regard to matches found

Identification process of an individual

Figure 1: Block diagrams of registration, verification, and identification process of biometric systems

A biometric system is effectively a prototype identification system that distinguishes an individual by an inimitable attribute vector resulting from a specific physiological or behavioral feature that the individual possesses. By relying on the usage context, a biometric structure usually functions for authentication, which typically delivers Boolean conclusion (authorized or not) or classification (identification, which typically identifies the operandi or operator.

In authentication approach, the structure authorizes an individual's identity by contrasting the incarcerated biometric feature with the individual's biometric pattern, which obtainable in the pattern database. In such a system, an individual who desires to be predictable (for example, Bob) claims an identity usually via a required features such as individual identification, login identity, card identity or the like, then the authentication process performs validation of features submitted. In this regard a dilemma still alive is, "Is ıis features submitted really by its actual owner?" Hence lentity recognition comes in the way to sort this issue, where ıe aim is to prevent more than one individual from using the ıme traits.

ı identification approach that clears the dilemma of "who is ıis individual?", the structure recognizes an individual by ·obing the entire pattern database for a match. The structure ırries out a one-to-many assessment to institute an ıdividual's distinctiveness. Identification is a significant ıctor of pessimistic recognition models, in which the structure institutes to identify that particular individual is block listed or banned. The purpose of pessimistic recognition is to avert a single individual from using numerous identities. Identification can also be used in optimistic identification for expediency. While the conventional methods of individual identification such as passwords, PINs, keys, and tokens work for optimistic identification, only biometrics can be used for pessimistic identification.

Figure 1 explores the authentication and identification structure, both requires the process of user registration. The registration module registers individuals into the biometric pattern database. During the conscription phase, a biometric reader first scans the individual's biometric characteristic to produce its digital representation. The structure generally performs a quality check to ensure that successive stages can reliably process the attained traits. To smooth the progress of corresponding, a trait collector practices the input trait to produce a condensed but communicative illustration, called a pattern. By relying on the context, the biometric structure may stock up the pattern in its pattern database or publish it on a smart card issued to the individual.

2.3 Biometric system errors

The traits submitted to Biometric structure is validated based on the matching score, since any two samples of traits submitted by one individual practically failed to be identical due to sensor noise, changes in physiological or behavioral features, temperature and humidity conditions, improper interaction during trait submission. Hence the biometric structure enumerates the compatibility between the traits submitted for validation and patterns available in database; the higher the score signifies the compatibility between traits submitted and patterns available in database. An accuracy threshold will be considered to evaluate the similarity scores. A similarity score above the accuracy threshold indicates pairing of the traits submitted and patterns in database

The distribution of pairing scores engendered from pairs of trait models from dissimilar individuals is called an charlatan division; the score division engendered from pairs of samples from the same individual is called a authentic division.

A biometric authentication scheme can falsify as biometric evaluation by concluding that trait samples from dissimilar individuals as trait samples of same individual that referred as false positive. Vice versa falsify as biometric evaluation by concluding that trait samples from same individual as trait samples of divergence individuals that referred as false negative.

Besides this other malfunction factors such as capturing malfunction (CM), registration malfunction (RM) also possible. These malfunction factors can be used to rate the biometric structure credibility. The CM rate is considerable automatic-capturing process, The CM rate denotes the failure percentage of the device that used for registration process.

2.4 Applications of biometric systems

Biometric structures categorized as commercial applications, such as computer network access authorizations, securing electronic data, e-commerce and Internet right of entry, Automatic Teller Machines, credit cards, physical access control, cellular phones, PDAs, EMR management, and E-learning; E-Governance related identity access, correctional amenities, licenses, social security, military operations and Forensic applications such as fraud detection corpse identification, criminal investigation, terrorist identification.

3. CONTEMPORARY AFFIRMATION OF BIOMETRICS BASED VERIFICATION AND IDENTIFICATION SYSTEMS IN RECENT LITERATURE

3.1 Privacy and Security Issues

The biometric traits of one individual taken during verification phase, most often failed to match with the traits submitted during the registration. This is due to the issues of noise produced during biometric traits collection, an injury to human organ that used to produce required traits or issue of aging. The other issue related to biometrics based security system is privacy leakage. The traits collected from one individual are processed in to a specific format and stores in a database, which is vulnerable to privacy leakage attack. An experiment explored in [27] proved that the finger prints stored in a minutiae format can reverse back to identify the user to whom that traits related. These biometric related traits need to be stored such a way that they are not vulnerable to privacy leakage, since these traits are unchangeable like in traditional password based systems.

In this regard many of solutions that aimed to avoid the privacy leakage can be found in recent literature. The models explored in [5][6][7] are secure sketch based standards. Here in this standard, during the registration phase, the collected biometric traits are converted to hash format and prepares some supporting data to recognize the actual traits from that hash format. The models devised in [8][9][10] are improved secure sketch based approaches. Unlike the models explored in [5][6][7] that are based on error control schemes, the models devised in [8][9][10] are based on practical coding schemes. The empirical study presented in [11] explored the security vulnerabilities of the models devised in [5][6][7][8][9][10]. A model devised in [12] is a biometric structure that transforms the biometric traits into irreversible transformation and stores in the database [13]. Some of the interesting models projected in [14][15][16][17][18], which are based on fuzzy vault scheme that let to extract keys from the biometric traits and encrypts that biometric traits submitted during registration phase and preserves encoded results into database. During the verification phase the same keys will be extracted from biometric traits submitted for authentication and decrypts the data in database. The qualitative analysis of these models explored in [19][20][21][22]. Protecting the biometric patterns using cryptography is another interesting factor that devised in [23].

Observation: In regard to qualitative analysis prospective, the fundamental strategy of these models engenders a key and supporting data from biometric traits submitted in registration phase. Then the key will be encoded into hash format and preserves the database along with the support data. During the verification phase, the similar process repeats that extracts key from the biometric traits submitted for verification, which may contain noise. Henceforth to identify the exact key this process utilizes the support data stored in database. Then it compares the hash format of the key extracted with hash format stored in database. The impact of noise observed along with biometric traits submitted for verification can be lessened by an error correction strategy. This error correction strategy mitigates the noise by using supporting data as the set of symptoms. In regard to improve this verification structure, the current research models aimed to maximize the rate of accuracy in deriving key from the biometric traits collected along with unavoidable noise. In a theoretical analysis perception, these secret key based approaches are still vulnerable to guess attacks that attempts to predict the actual key [24][25][26], and henceforth the key length is maximized [21] to avoid this guess attacks. In the context key, it might be secure according to the length of the key, but the supporting data can compromise to deliver the actual biometric traits. The process of maximizing the key rate theoretically proposed to avoid vulnerabilities but they do not address the concerns related to privacy in effectual manner. In qualitative vision, the supporting data that can compromise to reveal the measuring parameters of the submitted traits is also need to be protective along side of the key rate maximization.

3.2 Identity leakage Issues:

The biometric traits format that preserved in database is predictable that vulnerable to various security threat. For instance, as discussed in previous section (3.A), the finger prints stored in a trivia format can reverse back to identify the user to whom that traits related and these traits are unchangeable like in traditional password based systems. Henceforth identity theft is possible in compromised conditions of the database. The biometric traits stored under poor confidential circumstances leads to serious Identity leakage. The cryptographic standards also not helpful to protect the confidentiality in conditions such as an authorized administrative individual can get access to decryption keys and may use it on his interests to leak the personal identity of the authorized user. The one way hashing approaches can help in this regard, where credentials of a user stored in database as one way hash format and compares with the one way hash format of the produced credentials during authentication process. But in the case of biometric traits often the devices used to collect these traits in any two iterations failed to collect them in identical passion. Since these biometric traits are not identical in any two submissions of one individual, which is due to changes in limb used for traits submission, erroneous submission by user or noise produced by Biometric devise. Hence the one way hash based verification techniques failed to work. In this regard many of the models projected in recent literature opting to a strategy that maps set of optimal values possible from an individual to one that preserved in database with privacy considerations. Some of the interesting models projected such as FCS1 [28], HDS2 [29], FE3 [30], FV 4[31], CB5 [32] and LA6 [33] [34], and these all models are centric to the verification process of individual, which is done by the mapping process that uses supporting data. These models are vulnerable to leak the identity since the compromised supporting data can reveal the user identity. This vulnerability is practical in conditions such as a fraudulent verification authority attempting to exploit this supporting data.

1Fuzzy Commitment Scheme

2Supporting data Scheme

3Fuzzy Extractors

4Fuzzy Vault

5Cancellable Biometrics

6Likelihood based Approaches

Since the biometric pattern protection is a serious research issue, the numerous structures can be found in recent literature. These models are fall in either trait transformations or in biometric cryptosystems [35].

The trait transformation achieves biometric traits and supporting data privacy by protecting the trait transformation features. Here in this strategy the biometric traits and their supporting data preserves in database in a novel transformation format that can be invertible by using the same transformation features. Henceforth the privacy of these biometric traits and supporting data is dependent on level of protection given to these transformation features [36]. Henceforth the inaccessibility due to missing or leakage of these transformation features leads to identity leakage [37]. In this context irreversible transformations [38] proposed, which depends on one way hash techniques.

In practice, figuring out the practical complexities and vulnerabilities of reversible transformation and reformation is difficult. A modal devised in [39] explored a process of human inspection. This modal is using the process of irreversible transformation to transform the face metaphors into patterns. In the similar passion a model devised in [40], which is dependent of irreversible transformation of Cartesian, polar, and functional details of fingerprint pattern. An irreversible transformation strategy is devised in [41], which is vulnerable to a "record multiplicity attack" that can be described as the access to more than one stored patterns leads to access the actual biometric traits [42]. An irreversible transformation approach projected in [43] is with a detailed security and renewability analysis.

The interrelation between cryptography and biometric systems is a dependent factor in Biometric cryptosystems. The structure defined under biometric crypto systems fall in either Key Generation Schemes (KGS) or Key Binding Schemes (KBS). In the KBS strategies the collected biometric traits integrated with keys selected under random choice. In contrast KGS evidence the advantage of creating multiple keys as a set with given biometric traits without depending on any external data, which result firm cryptographic key [44]. These KGS systems scalability in regard to recognition is low, which is due to the variations in biometric traits submitted for validation [45].

The binary key used in a KBS system protects a derived biometric pattern in regard to achieve the confidentiality of a biometric identification structure, and relies on a biometric trait of an individual to reveal the related cryptographic key. Henceforth these KBS systems are referred as twofold authentication strategies. The secret key derived in KBS is not dependent of biometric traits used and uses to produce supporting data. This secret key shared with the authorized user through the reference pattern at registration phase. Henceforth it locks the privacy of biometric traits and cryptographic key in optimal manner. During the authentication phase, this supporting data will be linked with biometric traits submitted. To achieve scalability in this biometric crypto systems, error correction strategies are used to handle the variations in biometric traits collected to correlate with preserved patterns. The considerable KBS modals projected in [47] [48] [49] [50] [51] are recommending the fuzzy commitment strategy that devised in [46]. The KBS modal devised in [53] [54] [55] is using the fuzzy vault scheme [52], which is proven to be vulnerable in an empirical study projected in [56]. In contrast to fuzzy commitment and fuzzy vault strategies related KBS models, an optimal KBS modal devised in [57], that binds binary keys with biometric traits using "QIM (Quantization Index Modulation)" in regard to achieve scalability in minimizing the variations in biometric traits submitted for authentication. Enrique Argones Rúa et al.,[58] presented a cross modal that exploits the features of "UBMs (Universal Background Models)" to achieve scalable protection for biometric patterns. The authors claimed these UBMs are significant since these UBMs produce statistical descriptions to signify user level autonomous biometric observations.

Observation: With regard to seclusion concerns in biometric based structures, trait transformation and biometric crypto strategies are emerged as quite significant with balanced pros and cons. In particular irreversible trait transformations are intricate to characterize and related to KBS strategies it is not scalable in all aspects to reform, since KBS strategies are supporting data dependents. The cross models [59] can reflect the benefits of trait transformation and biometric cryptography strategies. Henceforth these cross models are in demand to fulfill the strategic needs to protect biometric patterns.

3.3 Visual Cryptographic Systems for Privacy in Biometrics

One of the well versed methodologies to defend biometric patterns [60] is cryptography. It is the ability of transfer and getting encrypted data that can be decrypted only by the source of the data or the authorized target of the data transmitted. Encryption and decryption are accomplished by using arithmetical algorithms in such a way that no one except the authorized individual can access the data by decrypting it. Naor and Shamir [61] devised the "visual cryptography scheme" (VCS) as an effortless and secure way to allow the secret sharing of metaphors without any cryptographic calculations. VCS is a cryptographic practice that permits to encrypt the visual information and decrypt by authorized individual visual system. The fundamental design is labeled as (K, n) VCS [61].

Nakajima and Yamaguchi [62] projected a 2-out-of-2 enhanced VCS for natural metaphors. They recommended a hypothetical structure for encoding a natural metaphor in innocuous metaphors as demonstrated in Figs. 2 and 3.

This is known as the "gray-level extended visual cryptography scheme" (GEVCS). In this work, the fundamental VCS are used to protect iris codes and fingerprint metaphors and the extended VCS for grayscale metaphors are used to secure face metaphors.

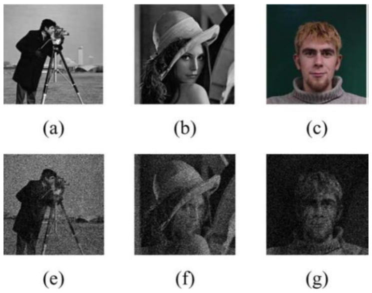


Fig. 2 [62]: Encryption of a private face metaphor in two standard host metaphors; (a) Host 1: Cameraman metaphor. (b) Host 2: Lena metaphor. (c) A private face metaphor. (e) and (f) The two host metaphors after visual encryption (two sheets). (g) Result of superimposing (e) and (f).

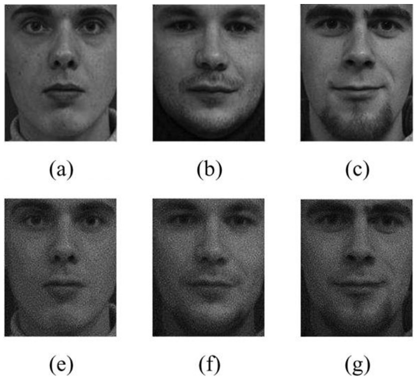


Fig. 3 [62]: Encryption of a private face metaphor in two pre aligned and cropped face metaphors. (a) and (b) are two host metaphors. (c) is a private face metaphor. (e) and (f) are the host metaphors after visual encryption (two sheets). (g) is the result of overlaying (e) and (f).

The use of fundamental visual cryptography for protecting fingerprint and iris patterns was suggested in [63] and [64], in that order; however, no experimental results were presented to reveal its effectiveness. Furthermore, fundamental VCS direct to the dilapidation in the eminence of the decoded metaphors, which makes it inappropriate for comparing process. The covering or superimposing process in visual cryptography is computationally sculpted as the binary OR process which origins the dissimilarity level of the target metaphor to be lowered. Loss in contrast in target metaphors could be addressed by simply substituting the OR operator with the XOR operator [65]. Furthermore, the target metaphor can be down-sampled by reconstructing just one pixel from every block. Thus, the reconstructed metaphor will be visually appealing while requiring less storage space.

Arun Ross et al., [66] explored the possibility of using visual cryptography for imparting privacy to biometric data such as fingerprint metaphors, iris codes, and face metaphors. This model is based on the process of decomposing the original metaphor into two metaphors in such a way that the original metaphor can be exposed merely when selected metaphors are simultaneously available; further, the individual component metaphors do not reveal any information about the original metaphor. In regard to registration the submitted confidential biometric traits will be sent to a trusted party. Upon receiving the confidential biometric traits, decomposes into set of two metaphors and then discards the original. Afterwards these decomposed metaphors will be stored into two divergent database servers such that theses servers even compromised, unable to trace the confidential data. In the course of verification, the trusted party collects related metaphors from data servers and overlaid the received related metaphors to restructure the confidential metaphor. This explored authentication process keeps away of complex decryption and decoding calculations used in [67], [68] [69] and [70] modals. Once the similarity score is worked out, the restructured metaphor is removed.

Observation: The issues that are seriously need to be considered during the usage of Visual Cryptography to deal with biometric privacy challenges:

The lucidities have to be acceptably associated in order for the message to be visible. Therefore the obstruction would be that the user cannot make use of diverse printers to produce the lucidities since diverse printers have dissimilar configuration setting.

In order to make sure privacy and protection, there is a requirement to "destroy physical evidence" in order to thwart the hazard of swindle, henceforth the originality of the message that retrieved from metaphors overlapping is often questionable.

3.4 Multimodal biometrics Based Authentication

The multimodal biometric systems offer significantly provides higher security in contrast to unimodal and fewer vulnerable to assails. The modal explored in [71] attempted to enhance the scalability of the practical biometric traits. In this regard the experiments conducted on multiple fixed blends of strategies. In the aim of high fortification, a multimodal approach projected in [72] that performs continuous verification of finger and face traits that collected and preserved. A multimodal structure projected in [73], which is based on dynamic matching scores from available matching scores. This dynamic selection of optimal matching score is based on the likelihood of user's legitimacy. A modal referred as BioID projected in [74] that aimed to explore divergent decision strategies on various biometric traits by manifold security stages. In this regard BioID performs much better by depending on administrator‘s choice of decision strategies. A reconciling usage of multimodal biometric approaches to achieve scalability and accuracy in biometric verification structure is devised in [75]. This modal opts to decision rules such that it can conclude the decisions from multiple biometric devices to meet the optimal performance. Another interesting multimodal biometric verification structure projected in [76]. This multimodal performs by including manifold blend of rules to guarantee anecdotal security necessities. This modal is using reconciling mishmashes of multimodal matching to handle the permissions in manifold manner. The performance of this multimodal [76] is determined to be advanced as evaluated to the decision-level scenarios.

Observation: In regard to model devised in [71], it is obvious to conclude that relying on fixed fusion strategies is optimal, since it has been shown in [77][78] that there is no significant advantage of using dynamic mishmashes over predetermined mishmashes. The approach explored in [72] demands the required biometric traits from the user. Henceforth this modal is not optimal and impractical for applications such as multilevel conditional authentication. The approach devised in [73] is not proven to be optimal since the accuracy is inconsistence. The multimodal devised in [74] may well enough to make a decision during required security level is low, in contrast its performance is suspicious for high security applications, as it is ambiguous and insistent to diverge the security levels. The work detailed in [75] is ought to be capable but failed to manage the optimality in authentication process, which is due to the uncertainty in decision level mishmashes and desired iterations are relatively very high. In addition, the information levels in this decision level mishmash are relatively very low that compared to other mishmashes such as trait mishmashes and match score mishmashes. Henceforth conceptual tags mishmash at decision level is not consistent in multimodal systems. In this regard, due to their ability of delivering more information, reconciling matching scores mishmash is a promising approach for multimodal strategies. In addition to the advantage of reconciling matching scores mishmash, the model devised in [75] is explored as Gaussian, which is optimal. The model devised in [76] is proven to be vulnerable to spoof attacks [79]. In particular the modal [76] is vulnerable, if trained by traditional learning algorithms with one biometric trait as input.

3.5 Using electrocardiogram (ECG) as biometric for Authentication

Through the deployment of ECG-enabled biometric system, the identity of an individual can be verified online during ECG monitoring or offline through the medical records. This identity verification is much more useful for the protection of individual identification and protection of his/her privacy about the cardiovascular condition in particular to the cardiovascular patients [80]. Although the methods of using ECG as a biometric possibly might not offer satisfactory correctness, but it has potential to supplement the information for a multimodal system. The inclusion of ECG to a multimodal system not only improves the system ac-curacy but also it improves the robustness of the system against non-live samples to be enrolled.

Israel et al. [81] demonstrated that ECG of an individual shows sign of inimitable pattern. A set of proven metrics were proposed to identify the uniqueness of heart beat of each individual. A set of fifteen intra-beat traits are noticed in cardiac functioning of each heart beat and categorized these traits by “linear discriminate analysis”. The experiments in [81] indicate that these intra-beat traits are not influenced by the placement of electrodes and stable in all states such as nervousness of each individual and universally inimitable.

A survey produced in [82] explored the earlier models that attempted to use features of ECG of an individual as biometric traits. The empirical study was explored with a set of 20 individuals. The initial experiments selected number of traits from each heart beat is 30. Further this set of traits reduced to 12 by analyzing the rank of correlation between these traits and discarded traits that are highly correlated. This set of 12 traits used further for multivariate analysis based classification. The plotting of PCA score is utilized to figure out the resemblance and divergence of heartbeats among individuals. Shen et al. [83] conducted the biometric experiment for identity verification using facade and time domain traits of the heartbeat. Since the usage of QRS average to extract traits from ECG wave provides the. Two neural network strategies related to pattern matching were used to enumerate the verification rates of individuals identity indicates the accuracy with an average of 82% and 97% in that order. The combination of these two strategies delivered 1005 accuracy for given set 20 individuals ECG waves as input.

The model devised in [84] is framework that uses ECG based biometric traits related to logical and facade. The critical feature incarcerate temporal and amplitude features of a heart beat and combines while the traits related to facade captures the functional related patterns in a heartbeat. To improve the usage of the balancing characteristics of decisive and facade traits, a multilevel biometric trait incorporation scheme is offered. A cross model, which is the combination of auto correlation and discrete cosine transform is devised that found to be accurate with an average of 96% to extract the selected biometric traits from ECG wave.

Recently, Singh and Gupta [85][86] explored the viability of using biometric traits extracted from ECG Wave of an individual to abet in biometric verification strategies. They outlined the ECG wave standard of each individual. The experiment results are found promising and scalable over other published methods. The proposed system is tested on 50 individual ECGs and the similarity between stored and collected ECG signals are identified by the process of correlation evaluation. The system is achieved the classification accuracy 98%.

Observation: Contrasting to usual biometrics that are neither secrets nor robust enough against falsification, ECG is inherited to an individual, which is highly secure and impossible to be forged. Most importantly, ECG has an inherent real-time feature of vitality signs which ensures that an ECG cannot be acquired unless the individual is not live or it cannot be acquired unless the individual to be authenticated is not present at the authentication desk. Therefore, it is robust enough against the falsified credentials to be enrolled in the system. We have shown that ECG has potential to provide an excellent source of supplementary information in a multimodal system. The fusion of ECG with the face biometric and with the fingerprint biometric has shown a significant improvement in authentication performance of both of the fused systems. In addition, we have critically examined the research concerns of ECG-enabled biometric authentication system across wide range of conditions. Upon the review of the authentication strategies[81][82][83][84][85][86], which are using ECG as biometric, we can conclude that These systems are not sufficient to perform the authentication task across wide range of conditions over a larger population including the data acquired at larger time intervals. And another practical issue that overlooked is what extent an ECG varies under different anxiety levels.

4. CONCLUSION:

Any system guarantees trustworthy individual identification ought to of necessity to entail a biometric module. And this biometrics expertise is a new technology for the majority of us for the reason that it has been employed in public for diminutive period of time. Since of the inimitable individual identification probable endowed with biometrics, they have and will persist to afford constructive worth by preventing crime, recognizing criminals, and abolishing swindle. Hence there are many structures of biometrics technology employed in security systems. It has numerous advantages such as improved security and effectiveness, abridged fraud and alleviative usage. At the same time, it is essential to control the problem of "function creep", encourage the structures that do not intimidate essential privileges to confidentiality and secrecy, and authenticate the business case for deployment. The domain of Biometrics is one of the significant and prospective in terms of future research due to its associated unique legal, political and business challenges. The other feature that observed in our contemporary affirmation of the recent literature is a less attention is given by current research domain on biometric based crypto systems and issues and challenges observed in adaptive biometric security with mobile devices. Hence our future research can attempt to devise scalable crypto systems that interrelated with mobile devises based adaptive biometrics.

REFERENCES

[1] Jain, A.K.;Ross, A.;Prabhakar, S.;"An introduction to biometric recognition", Volume: 14 Issue: 1 Issue Date: Jan. 2004, on page(s): 4 - 20
[2]Jain, A.K.; Ross, A.; Pankanti, S., "Biometrics: a tool for information security" Volume: 1 Issue: 2, Issue Date: June 2006, page(s): 125 - 143
[3] Michael E. Schuckers, "Some Statistical Aspects of Biometric Identification Device Performance", 2001
[4] Sandra Maestre, Sean Nichols "DNA Biometrics", 2009
[5] Y. Sutcu, Q. Li, and N. Memon, "Protecting biometric patterns with sketch: Theory and practice," IEEE Trans. Inf. Forensics Security, vol. 2, no. 3, pp. 503–512, Sep. 2007.
[6] Q. Li, Y. Sutcu, and N. Memon, "Secure sketch for biometric patterns," in Proc. Asiacrypt, Shanghai, China, Dec. 2006, pp. 99–113.
[7] Y. Sutcu, Q. Li, and N. Memon, "Secure biometric patterns from fingerprint- face features," in Proc. IEEE Computer Society Workshop on Biometrics, Minneapolis, MN, Jun. 2007.
[8] S. Draper, A. Khisti, E. Martinian, A. Vetro, and J. Yedidia, "Using distributed source coding to secure fingerprint biometrics," in Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing, Honolulu, HI, Apr. 2007, pp. 129–132.
[9] Y. Sutcu, S. Rane, J. S.Yedidia, S. Draper, and A.Vetro, "Feature transformation of biometric patterns for secure biometric systems based on error correcting codes," in Proc. IEEE Conf. Computer Vision and Pattern Recognition, Anchorage, AK, June 2008.
[10] G. Davida, Y. Frankel, and B. Matt, "On enabling secure applications through off-line biometric identifications," in Proc. IEEE Symp. Security and Privacy, Oakland, CA, May 1998, pp. 148–157.
[11] K. Simoens, P. Tuyls, and B. Preneel, "Privacy weaknesses in biometric sketches," in Proc. IEEE Int. Symp. Security and Privacy, May 2009, pp. 188–203.
[12] J. Bringer, H. Chabannea, and B. Kindarji, "The best of both worlds: Applying secure sketches to cancelable biometrics," Sci. Comput. Program., vol. 74, pp. 43–51, 2008.
[13] N. Ratha, S. Chikkerur, J. Connell, and R. Bolle, "Generating cancelable fingerprint patterns," IEEE Trans. Pattern Anal. Mach. Intell., vol. 29, no. 4, pp. 561–572, Apr. 2007.
[14] X. Boyen, "Reusable cryptographic fuzzy extractors," in Proc. ACM Conf. Computer and Communications Security, New York, 2004, pp. 82–91, ACM Press.
[15] A. Juels and M. Sudan, "A fuzzy vault scheme," in Proc. IEEE Int. Symp. Inform. Theory, Lausanne, Switzerland, Jun./Jul. 2002, pp. 293–297.
[16] U. Uludag, S. Pankanti, and A. K. Jain, "Fuzzy vault for fingerprints," Audio- and Video-Based Biometric Individual Authentication, pp. 310–319, Jul. 2005.

[17] U. Uludag and A. K. Jain, “Securing fingerprint pattern: Fuzzy vault with supporting data,” in Proc. IEEEWorkshop Privacy Research in Vision, New York, 2006.

[18] Y. Dodis, L. Reyzin, and A. Smith, “Fuzzy extractors: How to generate strong keys from biometrics and other noisy data,” in Proc. Advances in Cryptology (EUROCRYPT), Interlaken, Switzerland, May 2004, pp. 523–540.

[19] G. Cohen and G. Zemor, “The wire-tap channel applied to biometrics,” in Proc. IEEE Int. Symp. Inf. Theory and Its Applications, Parma, Italy, Oct. 2004.

[20] T. Ignatenko and F. M. J. Willems, “On privacy in secure biometrics authentication systems,” in Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing, Honolulu, HI, Apr. 2007, pp. 121–124.

[21] P. Tuyls and J. Goseling, “Capacity and examples of pattern-protecting biometric authentication systems,” in Biometric Authentication. Berlin, Germany: Springer, 2004, pp. 158–170.

[22] A. Nagar, K. Nandakumar, and A. K. Jain, “Biometric pattern transformation: A security analysis,” in Proc. SPIE, Electronic Imaging, Media Forensics and Security, San Jose, Jan. 2010.

[23] M. Upmanyu, A. M. Namboodiri, K. Srinathan, and C. V. Jawahar, “Efficient biometric verification in encrypted domain,” in Proc. Int. Conf. Biometrics, Sassari, Italy, 2009.

[24] U. M. Maurer, “Secret key agreement by public discussion from common information,” IEEE Trans. Inf. Theory, vol. 39, no. 3, pp. 733–742, May 1993.

[25] R. Ahlswede and I. Csiszár, “Common randomness in information theory and cryptography, Part I: Secret sharing,” IEEE Trans. Inf. Theory, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.

[26] R. Ahlswede and I. Csiszár, “Common randomness in information theory and cryptography, Part II: CR capacity,” IEEE Trans. Inf. Theory, vol. 44, no. 1, pp. 225–240, Jan. 1998.

[27] A. Ross, J. Shah, and A. K. Jain, “From pattern to image: Reconstructing fingerprints from minutiae points,” IEEE Trans. Pattern Anal. Mach. Intell., vol. 29, no. 4, pp. 544–560, Apr. 2007.

[28] A. Juels and M. Wattenberg, “A fuzzy commitment scheme,” in CCS ’99: Proceedings of the 6th ACM conference on Computer and communications security, 1999.

[29] J.-P. Linnartz and P. Tuyls, “New shielding functions to enhance privacy and prevent misuse of biometric patterns,” in Audio- and Video-Based Biometric Individual Authentication. Springer Berlin / Heidelberg, 2003.

[30] Y. Dodis, L. Reyzin, and A. Smith, “Fuzzy extractors: How to generate strong keys from biometrics and other noisy data,” in Lect Notes Comput Sc. Springer Berlin / Heidelberg, 2004.

[31] A. Juels and M. Sudan, “A fuzzy vault scheme,” Design Code Cryptogr, vol. 38, pp. 237–257, 2006.

[32] N.K. Ratha, S. Chikkerur, J.H. Connell, and R.M. Bolle, “Generating cancelable fingerprint patterns,” IEEE T Pattern Anal, vol. 29, pp. 561 – 572, 2007.

[33] A.M. Bazen and R.N.J. Veldhuis, “Likelihood-ratiobased biometric verification,” IEEE T Circ Syst Vid, vol. 14, pp. 86 – 94, 2004.

[34] C. Chen, R.N.J. Veldhuis, T.A.M. Kevenaar, and A.H.M. Akkermans, “Multi-bits biometric string generation based on the likelihood ratio,” in Proc. IEEE Int. Conf. on Biometrics: Theory, Applications, and Systems, 2007.

[35] A. K. Jain, K. Nandakumar, and A. Nagar, “Biometric pattern security,” Special Issue on Biometrics, EURASIP J. Adv. Signal Process., pp. 1–17, Jan. 2008.

[36] A. B. J. Teoh, D. C. L.Ngo, and A.Goh, “Randommultispace quantization as an analytic mechanism for biohashing of biometric and random identity inputs,” IEEE Trans. PAMI, vol. 28, no. 12, pp. 1892–1901, Dec. 2006.

[37] S. Jassim, H. Al-Assam, and H. Sellahewa, “Improving performance and security of biometrics using efficient and stable random projection techniques,” in Proc. Int. Symp. Image and Signal Processing and Analysis (ISPA), 2003, pp. 556–561.

[38] N. K. Ratha, J.H. Connell, and R. Bolle, “Enhancing security and privacy of biometric-based authentication systems,” IBM Syst. J., vol. 40, no. 3, pp. 614–634, 2001.

[39] H. Lee, C. Lee, J. y. Choi, J. Kim, and J. Kim, “Changeable face representations suitable for human recognition,” Lecture Notes Comput. Sci., vol. 4642, pp. 557–565, 2007.

[40] N. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, “Generating cancelable fingerprint patterns,” IEEE Trans. Pattern Anal. Mach. Intell., vol. 29, no. 4, pp. 561–572, Apr. 2007.

[41] T. E. Boult, W. J. Schreirer, and R. Woodworth, “Revocable fingerprint biotokens: Accuracy and security analysis,” in Proc. IEEE Conf. Computer Vision and Pattern Recognition, Jun. 2007, pp. 1–8.

[42] F.Quan, S. Fei, C.Anni, andZ.Feifei, “Cracking cancelable fingerprint pattern of ratha,” in Proc. Int. Symp. Computer Science and Computational Technology, Dec. 2008, pp. 572–575.

[43] E. Maiorana, P. Campisi, J. Fierrez, J. Ortega-Garcia, and A. Neri, “Cancelable patterns for sequence-based biometrics with application to on-line signature recognition,” IEEE Trans. Syst., Man, Cybern. A, Syst., Humans, vol. 40, no. 3, pp. 525–538, Mar. 2010.

[44] Y. Dodis, L. Reyzina, and A. Smith, “Fuzzy extractors: How to generate strong keys from biometrics and other noisy data,” Lecture Notes Comput. Sci., vol. 3027, pp. 523–540, 2004.

[45] Y. Sutcu, Q. Li, and N. Memon, “Protecting biometric patterns with sketch: Theory and practice,” IEEE Trans. Inf. Forensics Security, vol. 2, no. 3, pp. 503–512, Sep. 2009.

[46] A. Juels and M. Wattenberg, “A fuzzy commitment scheme,” in Proc. 6th ACM Conf. Computer and Communication Security, Nov. 1999, pp. 28–36.

[47] P. Tuyls, E. Verbitsky, T. Ignatenko, D. Schobben, and T. H. Akkermans, “Privacy protected biometric patterns: Acoustic ear identification,” Proc. SPIE, vol. 5404, pp. 176–182, 2004.

[48] P. Tuyls, A. Akkermans, T. Kevenaar, G. J. Schrijen, A. Bazen, and R. Veldhuis, “Practical biometric pattern protection system based on reliable components,” in Proc. Audio and Video Based Biometric Individual Authentication (AVBPA), 2005, pp. 436–446.

[49] M. Van der Veen, T. Kevenaar, G.-J. Schrijen, T. H. Akkermans, and F. Zuo, “Face biometrics with renewable patterns,” in Proc. SPIE Security, Steganography, and Watermarking of Multimedia Contents, 2006, vol. 6072, pp. 205–216.

[50] F. Hao, R. Anderson, and J. Daugman, “Combining crypto with biometrics effectively,” IEEE Trans. Comput., vol. 55, no. 9, pp. 1081–1088, Sep. 2006.

[51] E. Maiorana, P. Campisi, and A. Neri, “User adaptive fuzzy commitment for signature patterns protection and renewability,” SPIE J. Electron. Imag., vol. 17, no. 1, pp. 1–12, Jan./Mar. 2008.

[52] A. Juels and M. Sudan, “A fuzzy vault scheme,” Designs, Codes, Cryptography, vol. 38, no. 2, pp. 237–257, 2006.

[53] M. R. Freire, J. Fierrez, M. Martinez-Diaz, and J. Ortega-Garcia, “On the applicability of off-line signatures to the fuzzy vault construction,” in Proc. Int. Conf.Document Analysis and Recognition (ICDAR), 2007, pp. 1173–1177.

[54] D. H. Nyang andK. H. Lee, “Fuzzy face vault: How to implement fuzzy vault with weighted features!!,” Lecture Notes Comput. Sci., vol. 4554, pp. 491–496, 2007.

[55] Y. J. Lee, K. Bae, S. J. Lee, K. R. Park, and J. Kim, “Biometric key binding: Fuzzy vault based on iris images,” Lecture Notes Comput. Sci., vol. 4642, pp. 800–808, 2007.

[56] W. J. Scheirer and T. E. Boult, “Cracking fuzzy vault and biometric encryption,” in Proc. IEEE Biometric Symp., Baltimore, MD, Sep. 2007.

[57] F. M. Bui, K. Martin, H. Lu, K. N. Plataniotis, and D. Hatzinakos, “Fuzzy key binding strategies based on quantization index modulation (QIM) for biometric encryption (BE) applications,” IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, pp. 118–132, Mar. 2010.

[58] Argones Rua, E.; Maiorana, E.; Alba Castro, J.L.; Campisi, P.; , "Biometric Pattern Protection Using Universal Background Models: An Application to Online Signature," Information Forensics and Security, IEEE Transactions on , vol.7, no.1, pp.269-282, Feb. 2012 doi: 10.1109/TIFS.2011.2168213 URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6020788&isnumber=6126191

[59] Y. C. Feng, P. C. Yuen, and A. K. Jain, “A hybrid approach for generating secure and discriminating face pattern,” IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, pp. 103–117, Mar. 2010.

[60] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy, and B. Kumar, “Biometric encryption,” in ICSA Guide to Cryptography. New York: Mc-Graw-Hill, 1999.

[61] M. Naor and A. Shamir, “Visual cryptography,” in Proc. EUROCRYPT, 1994, pp. 1–12.

[62] M. Nakajima and Y. Yamaguchi, “Extended visual cryptography for natural images,” J. WSCG, vol. 10, no. 2, pp. 303–310, 2002.

[63] Y. Rao, Y. Sukonkina, C. Bhagwati, and U. Singh, “Fingerprint based authentication application using visual cryptography methods (improved id card),” in Proc. IEEE Region 10 Conf., Nov. 2008, pp. 1–5.

[64] P. Revenkar, A. Anjum, and W. Gandhare, “Secure iris authentication using visual cryptography,” Int. J. Comput. Sci. (IJCSIS), vol. 7, no. 3, pp. 217–221, Mar. 2010.

[65] D. Jin, W.-Q. Yan, and M. S. Kankanhalli, “Progressive color visual cryptography,” J. Electron. Imag. vol. 14, no. 3, p. 033019, 2005
[Online]. Available: http://link.aip.org/link/?JEI/14/033019/1

[66] Ross, A.; Othman, A.; , "Visual Cryptography for Biometric Privacy," Information Forensics and Security, IEEE Transactions on , vol.6, no.1, pp.70-81, March 2011 doi: 10.1109/TIFS.2010.2097252 URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5658142&isnumber=5712892

[67] A. Jain and U. Uludag, “Hiding biometric data,” IEEE Trans. Pattern Anal. Mach. Intell., vol. 25, no. 11, pp. 1494–1498, Nov. 2003.

[68] J. Dong and T. Tan, “Effects of watermarking on iris recognition performance,” in Proc. 10th Int. Conf. Control, Automation, Robotics and Vision, 2008 (ICARCV 2008), 2008, pp. 1156–1161.

[69] N. Agrawal and M. Savvides, “Biometric data hiding: A 3 factor authentication approach to verify identity with a single image using steganography, encryption and matching,” in Proc. Computer Vision and Pattern Recognition Workshop, 2009, vol. 0, pp. 85–92.

[70] A. Jain, K. Nandakumar, and A. Nagar, “Biometric pattern security,” EURASIP J. Advances Signal Process., pp. 1–17, 2008.

[71] J. Kittler, M. Hatef, R. P. W. Duin, and J. Matas, “On combining classifiers,” IEEE Trans. Patt. Anal. Machine Intell., vol. 20, pp. 226-239, Mar. 1998.

[72] T. Sim, S. Zhang, R. Janakiraman and S. Kumar, “Continuous verification using multimodal biometrics,” IEEE Trans. Patt. Anal. Machine Intell., vol. 29, no. 4, pp. 687-700, Apr. 2007.

[73] R. Tronci, G. Giacinto, F. Roli, “Dynamic Score Selection for Fusion of Multiple Biometric Matchers”, Proc. 14th IEEE International Conference on Image Analysis and Processing, ICIAP 2007, Modena, Italy, pp. 15-20, 2007.

[74] R. W. Frischholz and U. Deickmann, “BioID: A multimodal biometric identification system,” IEEE Comput., vol. 33, no. 2, Feb. 2000.

[75] K. Veeramachaneni, L. A. Osadciw, P. K. Varshney, “An Adaptive Multimodal Biometric Management Algorithm,” IEEE Trans. Sys. Man & Cybern., Part-C, vol. 35, no. 3, pp. 344-356, Aug. 2005.

[76]Kumar, A.; Kanhangad, V.; Zhang, D.; , "A New Framework for Adaptive Multimodal Biometrics Management," Information Forensics and Security, IEEE Transactions on , vol.5, no.1, pp.92-102, March 2010 doi: 10.1109/TIFS.2009.2031892 URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5412146&isnumber=5412136

[77] D. M. J. Tax, M. V. Breukelen, R. P. W. Duin, and J. Kittler, “Combining multiple classifiers by averaging or multiplying,” Pattern Recognition, vol. 33, pp. 1475-1485, 2000.

[78] F. Roli, S. Raudys, and G. L. Marcialis, “An experimental comparison of fixed and trained fusion rules for crisp classifier outputs,” 3rd Intl. Workshop on Multiple Classifier Systems, MCS 2002, Cagliari (Italy), Springer-Verlag, LNCS, Jun. 2002.

[79]Zahid Akhtar, and Nasir Alfarid; Secure Learning Algorithm for Multimodal Biometric Systems against Spoof Attacks; 2011 International Conference on Information and Network Technology IACSIT Press, Singapore;IPCSIT vol.4 (2011) © (2011)

[80] F. Sufi and I. Khalil, “An Automated Patient Authentica-tion System for Remote Telecardiology,” Proceedings of the Fourth International Conference on Intelligent Sen-sors, Sensor Networks and Information Processing, ISS-NIP 2008, 15-18 December 2008, pp. 279-284.

[81] S. A. Israel, J. M. Irvine, A. Cheng, M. D. Wiederhold and B. K. Wiederhold, “ECG to Identify Individuals,” Pattern Recognition, Vol. 38, No. 1, 2005, pp. 133-142. doi:10.1016/j.patcog.2004.05.014

[82] L. Biel, O. Pettersson, L. Philipson and P. Wide, “ECG Analysis: A New Approach in Human Identification,” IEEE Transaction on Instrumentation and Measurement, Vol. 50, No. 3, 2001, pp. 808-812. doi:10.1109/19.930458

[83] T. W. Shen, W. J. Tompkins and Y. H. Hu, “One-Lead ECG for Identity Verification,” Proceedings of the Sec-ond Joint EMBS/BMES Conference, Houston, 23-26 Oc-tober 2002, pp. 62-63.

[84] Y. Wang, F. Agrafioti, D. Hatzinakos and K. N. Platani-otis, “Analysis of Human Electrocardiogram for Biomet-ric Recognition,” EURASIP Journal on Advances in Sig-nal Processing, Vol. 2008, 2008, Article ID: 148658, pp. 1-11.

[85] Y. N. Singh and P. Gupta, “Biometric Method for Human Identification Using Electrocardiogram,” Proceedings of the 3rd IAPR/IEEE International Conference on Biomet-rics, ICB 2009, LNCS, Springer-Verlag, Berlin, Vol. 5558, 2009, pp. 1270-1279.

[86] Y. N. Singh and P. Gupta, “Correlation Based Classifica-tion of Heartbeats for Individual Identification,” Journal of Soft Computing, Vol. 15, No. 3, 2011, pp. 449-460. doi:10.1007/s00500-009-0525-y