A Novel Biometric Technique Benchmark Analysis For Selection Of Best Biometric Modality And Template Generation Method

Raikoti Sharanabasappa11 *sr.raikoti@gmail.com*
Research Scholar Dravidian University
Kuppam, India

Dr Sanjaypande M. B.2 *rkroop99@gmail.com*
Prof. and Head of Dept.
VVIET Mysore, India

Abstract

A biometric security is a technique by means of which digital contents are protected by a cryptographic key generated from the biometric features of a person like Retina, Iris, Fingerprint, Face, Voice and so on. Normally the digital contents like documents are protected by a cryptographic key generated from a unique password. The process in irreversible, i.e the key can be generated from the password but not the vice versa. Passwords are relatively easy to hack as most of the users keep their personal information like date of birth as password and also password length has a limit as human beings cannot remember a password of significantly large length. Hence guessing the password of a user, whose significant information is available, is easier. Therefore off late lot of emphasis has been given to biometric features. Biometric features of no two people are same. For example the finger prints or the face of any two people differ. Hence if a template (alphanumeric or binary representation of features from a biometric data) is selected for the key generation than cracking them for accessing information becomes significantly difficult. But as with every advantage comes certain limitations also. The keys are not time invariant. Templates tends to change based on the data acquisition, or with time. For example the finger prints or palm prints changes with ages. Iris, retina and face features changes with change in light intensity during the acquisition phase. Fingerprint features changes with change in the orientation of the finger while scanning. In a classic authentication problem, such variability's can be easily dealt with by keeping a threshold for the acceptance of the features. Such acceptance threshold is not applicable for the case of biometric templates. Even slightest of the variability in the templates changes the generated key, therefore causing a high false rejection rate. Hence in this work we analyze the most accepted biometric features and techniques for key generation and propose the most invariable technique in terms of data acquisition invariability. The work analyzes Iris, Face, Fingerprint and Palm prints for analysis of the biometric template generation and key generation form the templates. Further a unique benchmark analysis technique is proposed for quantifying the quality of a biometric model or features.

Keywords: Template Quality Analysis, Biometric Security, Biometric Key Invariability.

1. INTRODUCTION

1.1 Public Key Cryptography

It is a means of exchanging digital data securely over a network or internet. If a peer wants to send a document to other peer by encrypting it, then the peers first exchange their secured keys. A key is unique number generated randomly using a key generation function with the help of a set of alphanumeric string and users identity (like user name). Hence the key is unique to each user. While peer A wants to send information to B, it encrypts the document with the public key of B. While decrypting, B needs to decrypt the document with its private key. Now even if there is an eavesdropping while the public keys are exchanged and unauthenticated user acquires the public key of B, any encrypted document transmitted from A to B will not be decrypted by the unauthenticated entity because it is unaware of the private key of B. Now if the same entity had to decrypt the document successfully, it has to “guess” the private key of B. It requires a reverse engineering by means of which the unauthenticated entity first tracks the function through which this key might have been generated and then uses a trial and error method to guess the key. A decade ago, this technique was quite full proof because the amount of time required by any computer to guess the key through trial and error method or as commonly known brute force method would be significantly high and extend to weeks and months. But Over the period of time the processing capabilities of the computers are being increased by many a folds. Therefore the random guessing of the keys has become less time consuming and hackers are able to crack most sophisticated keys even with the help of a simple personal computer and without the aid of any super computer. Hence there was a need to come up with techniques which offers more randomness than the unique string which used to be use as a key generation base. Hence biometric templates got an edge and attention for public key cryptography over last decade or so.

1.2 Biometric Templates

For generating the key it is essential to select a password as discussed in the previous section. A password is a typical and known combination of numerals and characters that user can remember. Now every user has a limitation of remembering the length of the password. Hence number of permutations is finite even though it is huge. Whenever possible combinations of the key are finite the probability of generating the key from random combination is non zero. Considering that there are ten digits and twenty six characters (English alphabet) and that the password is of length ten, then total possible combinations are ${}^{35}P_{10}$.

Now let us consider that number of possible symbol is S and the length of the password is D then possible combination C is depicted as

$C={}^{S}P_{D}$ (1)

Hence the randomness of the key can be increased by increasing the both S and D. Number of characters are fixed and is a set of maximum 256(as used by modern computer systems). Still it does not guarantee an infinite set. Instead of the symbols if real number sets are used as the base for generating the key than S becomes a set of all real numbers and can be claimed computationally infinite. Hence even a fixed length of D ensures a virtually untraceable key. It is almost impossible for human beings to remember large set of real numbers. Therefore a simple solution to the problem is to generate this number each and every time from the identity of the user, for instance face or fingerprint or palm print or voice or retina and so on. These identities are called biometric identities. The identity is scanned to a digital format and features are extracted from the pattern. These features are unique and are commonly known as biometric templates. A common technique for using these templates is to store them either centrally in a server or locally in the form of a smart card.

Hence a biometric template is a finite length set of either real numbers or symbols representing the unique identity of a person and can be used to generate unique key for public key cryptography [1].

Hence it can be said that biometric templates are set of measurable features which can be either used for public key cryptography or authenticating the person.

1.3 Problem formation

The biometrics features must be selected in such a way that it produces a unique and finite set for the user identity [2].

The overall process of data security can be elaborated in figure 1.

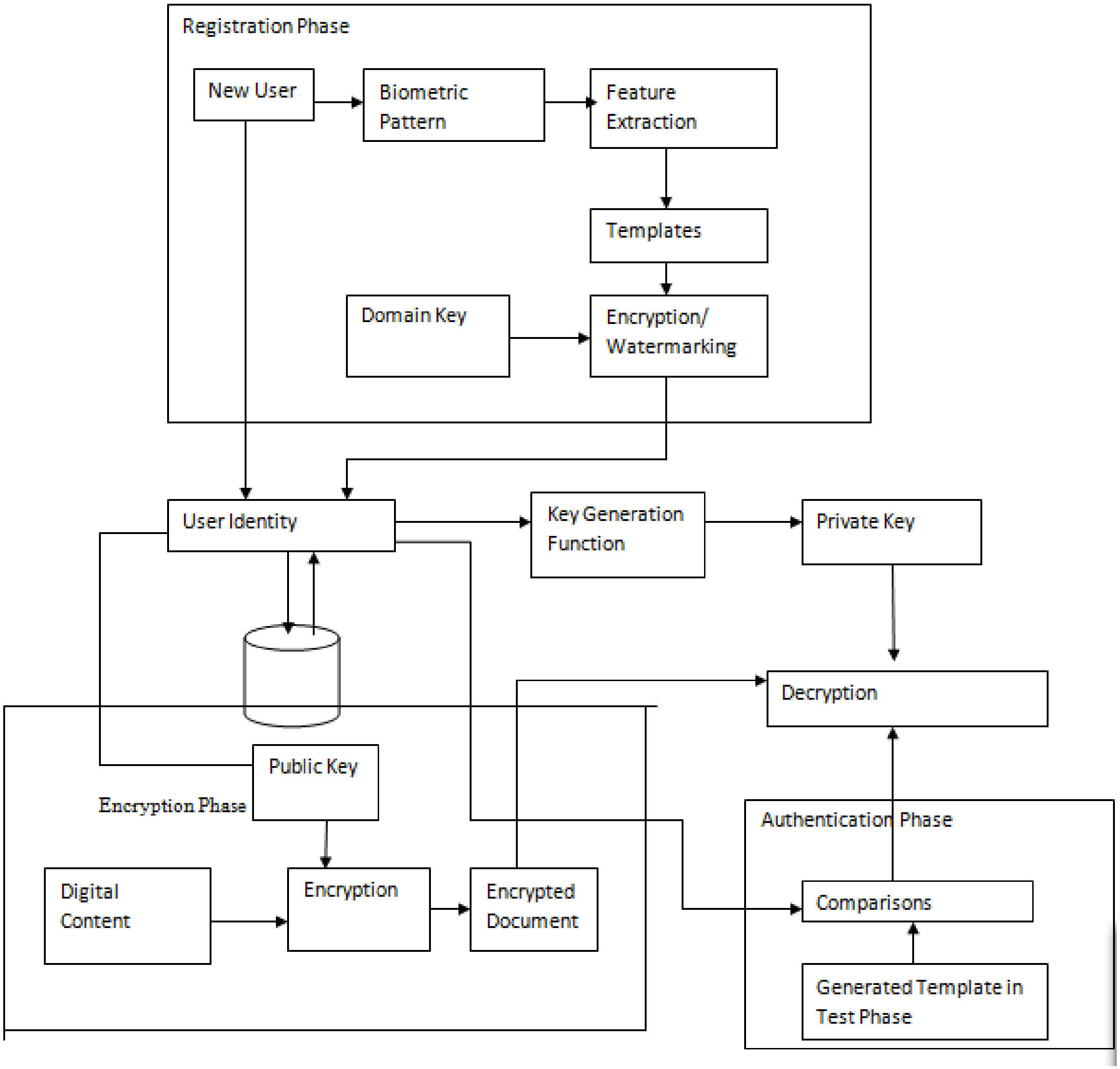

FIGURE 1: Biometric Template based public key cryptography.

When the user is registered for the first time, biometric template is extracted and stored in a database. When user receives an encrypted document which he needs to decrypt, he needs to get authenticated first. In authentication process biometric template of the user is regenerated and is compared with the features of the database and if they match the private key is generated from the stored features because every time new features are generated, they will not be 100% same as that of the stored templates. In key generation even deviation of a symbol out of a matrix of size say 1024, will result in generating wrong key. Hence the best method is to generate the key from the stored vector rather than the new vector. Further the stored vectors are protected using either watermarking techniques or are encrypted by a common domain key and are stored. Therefore if an unauthenticated intruder can track the domain key, he can easily temper with the stored key. Therefore the strength of the technique is considered to be dependent on the techniques of protecting the templates themselves, which interns minimizes the strength of the biometric templates itself.

A possible alternative to this problem is to device a mechanism by means of which it is not required to store the key in the database. Every time a document arrives, user's biometric

template is generated and a private key is generated from recently generated template rather than the existing stored template.
The solution is depicted in simple block diagram in figure 2.

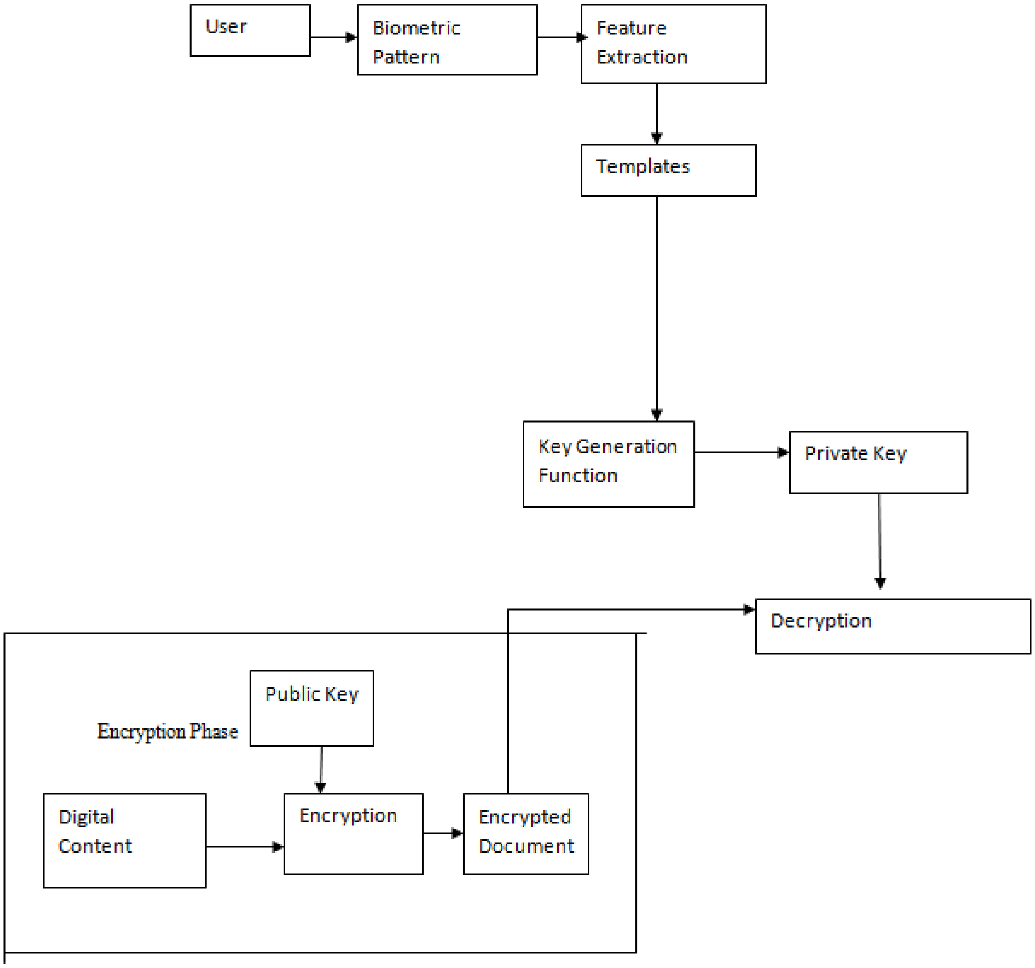

FIGURE 2: Proposed solution for Biometric security of the digital document.

Figure 2 clearly elaborates that there are no stored element to temper with. Therefore theoretically the key generated out of this technique is temper proof.
The main challenge with this technique is the variability of the features. Every time biometric data is acquired, it must be unique and the selected function must be such that it produces the exact key at every instance. Thus the first step is to find out the most invariant biometric features and template generation methods.

2. BENCHMARK ANALYSIS OF BIOMETRIC TEMPLATE SECURITY AND INVARIABILITY

2.1 Similarity With Self (SS)[2]

It is the average of the similarity scores obtained in the comparison between the user and the different access he has made. The greater the value, the more accurate is the biometric trait. A large value indicates similarity between the different stored versions of the user's biometric trait. This large similarity score overcomes the threshold. Maximization of this value reduces the false non match rate (FNMR).

SS must be very high and ideally 100% for every instance of template generation in order to ensure a unique key generation every time. Though with the current systems, it is not yet being achieved, this work towards identifying the biometric features and techniques to generate invariant features is to achieve this objective.

Let $s(x, y)$ be the matching similarity score between users x and y , given N genuine users,

$G_1, G_2, ..., G_n$ and $P(i)$ successful and genuine access of user i, $A(i)_1, A(i)_2, ..., A(i)_{P(i)}$ we

define $SS(Gi)$ as:

$$SS(Gi) = \frac{\sum_{j=1}^{j=P(i)} s(Gi, A(i)j)}{P(i)} \quad ...(2)$$

2.2 Similarity With Others(SO)[2]

Similarity with the other users *(SO – Similarity Others)*: is the average of the similarity scores obtained in the comparison between the user and the rest of the users stored in the database and the users found in the impostor access list. The smaller the value, the more accurate is the biometric trait. A small value indicates a great distinction with the rest of the users stored in the database and potential impostors. This small similarity score doesn’t overcome the threshold. Minimization of this value reduces the false match rate (FMR). Even though the objective of this work is study the invariability amongst the templates of a users subsequent template acquisition and not authentication, Similarity with others gives a benchmark for analyzing how strong a particular technique is. The more the value of SO, the stronger the technique is considered.

Let $s(x, y)$ be the matching similarity score between users x and y , given N genuine users,

$G_1, G_2, ..., G_n$ and M impostors $I_1, I_2, ..., I_m$,we define $SO(Gi)$ as:

$$SO(Gi) = \frac{\sum_{j=1.j\neq 1}^{j=N} s(Gi, Gj) + \sum_{k=1}^{k=M} s(Gi, Ij)}{N+M} \quad ...(3)$$

2.3 Entropy Based Measures [3] and Guessing Distance

One of the most analytical measures for the quality of the biometric key is Strong Biometric Privacy (SBP) analysis. This explains that if an adversary learns no useful information about a biometric, given auxiliary information, the template used to derive the key, and the key itself. For instance, no computationally bounded adversary should be able to compute any function of the biometric.

This is a direct function of Key Randomness (KR). This elaborates the randomness of the generated keys to any adversary who has access to auxiliary information and the template used to derive the key. For instance, we might require that the key be statistically or computationally indistinguishable from random.

Randomness can further be analytically defined as the probabilistic variations in keys generated from user to user. Such probabilistic measures are elaborated by entropy measures.

Theoretical approaches begin by assuming that the biometrics has high adversarial min-entropy (i.e., conditioned on all the auxiliary information available to an adversary, the entropy of the biometric is still high) and then proceed to distill this entropy into a key that is statistically close to uniform.

However, in practice, it is not always clear how to estimate the uncertainty of a biometric. In more practical settings, guessing entropy [7] has been used to measure the strength of keys.
It is shown that the average number of successive guesses, $E(G)$, required with an optimum Strategy until one correctly guesses the value of a discrete random X , is under bounded by the entropy H(X) in the manner

$$E[G] \geq \frac{1}{4} 2^{H(x)} + 1 \ldots (4)$$

Provided that $H(x)$ 2 bits, this bound is tight within a factor of (4/e) when X is geometrically distributed. It is further shown that $E[G]_q$ may be arbitrarily large when $H(x)$ is an arbitrarily small positive number EO that there is no interesting upper bound on $E[G]$ in terms of $H(x)$.

We assume that a specific user u induces a distribution U over a finite, n-element set Ω. We also assume that an adversary has access to population statistics that also induce a distribution, P, over Ω. P could be computed from the distributions of other users u'!= u. We seek to quantify how useful P is at predicting U.

Let $\omega^* = \arg\max_{\omega \in \Omega} u(\omega)$. Let $L_P = (\omega_1, \ldots, \omega_n)$ be the elements of Ω ordered such that $P(\omega_i) \geq P(\omega_{i+1}) \, for \ all \ i \in [1, n-1]$. Define t^- and t^+ to be the smallest index and largest index i
such that $\left| P(\omega_i) - P(\omega^*) \right| \leq \delta$. The Guessing Distance between U and P with tolerance δ is defined as:

$$GD_\delta(u, p) = \log \frac{t^- + t^+}{2} \ldots (5)$$

2.4 Distance Measurement Techniques

2.4.1 Euclidian Distance

Most common and widely used distance measurement technique is Euclidian distance and is

given by

$$d_{Eucl} = \left\| v - c \right\|^2 \ldots (6)$$

Where is the test vector and is the template vector corresponding to class . The Euclidean distance treats all elements of the feature vector as equally important and uncorrelated.

2.4.2 Posterior Probability

In [9], it is claimed that decisions that are based on the posterior probability densities are optimal, where optimality means minimal error rates. An error rate can be calculated based on either a single user scenario or a multi user scenario. In this context, optimality is defined as the lowest FAR for a given FRR or alternatively the lowest FRR for a given FAR. Where FAR and FRR are the most common measures of the performance of biometric authentication system and are defined by Rate of (or Percentage of) False authentication for a worng user and rate of False non authentication or rejection of a correct user. Thus posterior probability measures elaborates wheather it is feasible to obtain certain desired optimality for the system.

The posterior probability density of class W given observed feature vector is given by

$$p(wv) = \frac{p(v \mid w).p(w)}{p(v)} \ldots (7)$$

where $p(v,w)$ is the probability density of the feature vectors given class w, $p(w)$ is the probability density of the class , and $p(v)$ is the prior probability density of the feature vectors. The feature vector is accepted as member of the template class if its posterior probability density exceeds a threshold $t \in [0, t_{\max}]$.

Thus it is important to define the rejection mechanism of a pattern along with its acceptance criteria.
It is known [I0] that the optimum rule is to reject the pattern if the maximum of the a posteriori probabilities is less than some threshold. More explicitly, the optimum recognition rule is given as

$$\delta(d_k \mid v) = 1 \qquad (k \neq 0)$$

i.e., to accept the pattern v for recognition and to identify it as of the kth pattern class whenever

$$p_k F(v \mid k) \geq p_i F(v \mid j) \quad \text{for all j=1,2,...,n} \quad (8)$$

And

$$p_k F(v \mid k) \geq (1-t) \sum_{i=1}^{n} p_i F(v \mid i) \ldots \quad (9)$$

To reject a pattern

$$\max_i [p_i F(v \mid i)] < (1-t) \sum_{i=1}^{n} p_i F(v \mid i) \ldots (10)$$

where v is the pattern vector, n is the number of classes, $(p_1, p_2, ..., p_n)$ is the a priori probability distribution of the classes, $F(v \mid i)$ is the conditional probability density for v given the ith class, $d_i(i\,!=0)$ is the decision that v is identified as of the ith class while d, is the decision to reject, and t is a constant between 0 and 1 $(0 \leq t \leq 1)$.

2.4.3 Quantization Error and Log Likelihood Ratio[4]

There bound be the difference amongst the templates generated from one instance to another instance. Therefore under no way practically invariable templates can be generated. In order to minimize this variability, a quantization based technique is adopted by different works. According to this system, rather than using the values generated from the templates to generate the key, the template values can be quantized to set of values.
In a one-dimensional feature space V the likelihood ratio of user is defined as:

$$L_\omega = \frac{G(v, \mu_\omega, \sigma_\omega)}{G(v, \mu_0, \sigma_o)} \ldots (11)$$

Where the numerator defined the background probability density function and the denominator defines the actual probability density function of a user.
In simple terms, The generated pattern from the biometric features are Quantized to their nearest values and the likihood probability defines the fraction of probability of the quantized set to the probability distribution function of the actual set.

2.4.4 Normalized Hamming Distance

The formulated templates are converted into zeros and ones and are matched and similarity scores are calculated. Bit-wise comparison of the templates is made and Hamming distance is calculated for every such comparison. This is achieved by doing successive bit wise “X-OR”ing and “AND”ing. To account for the rotational inconsistencies the maximum matched value is chosen. The mask templates are used to ignore the noisy parts of the image. The formula for finding out the hamming distance is given as

$$HD = \frac{(codeA \otimes codeB) \cap maskA \cap maskB}{maskA \cap maskB} \quad \textbf{(12)}$$

2.5 Ratio of Bit Error Rate v/s Template Length[5]

It is fundamentally impossible to avoid noise during biometric data acquisition, because “life means change“. For example, faces age and iris patterns are not perfectly invariant to a contraction of a pupil. More noise is introduced by changes in the environmental conditions, which is again an unavoidable circumstance. Finally noise often finds its way into the sensor, during transmission or in the data processing process (“algorithmic noise“).

Thus noise removal from the templates must be considered an essential stage of biometric key generation.

The error corrected template is a *”bit identical“ unique data set that can be derived repeatedly from the different noisy biometric templates of a user*.

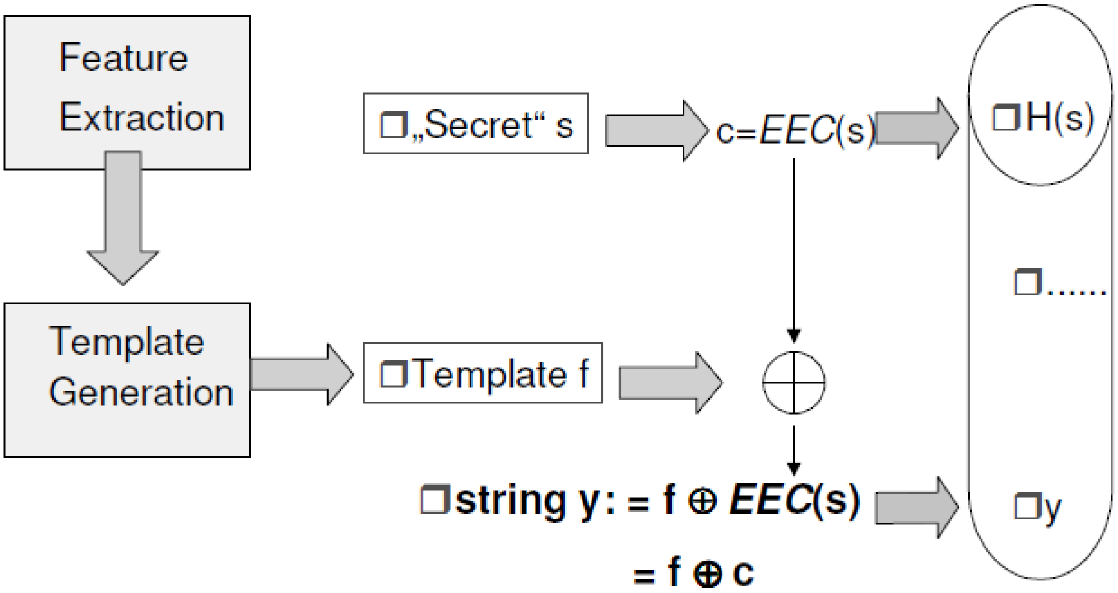

FIGURE 3: Biometric Key generation technique as par[11]

Juels and Wattenberg [18] proposed a very simple scheme based on any binary (not necessarily linear) [*n, k,* 2*t* +1] error correcting code *C* (+) GF(q)*n* for the Hamming distance with generator matrix G, where GF(q)*n* denotes the finite field with q elements. The encoding function transforms messages consisting of k symbols into n symbol code words (n>k), that can be retransformed into the original messages even if up to t symbols of the received codeword are corrupted due to error.

During enrolment, a random codeword, i.e. *c = G(s)* for a random *s* (+) GF(q)*k*, is bitwise added (XOR) to the biometric template *f* and the result is stored in the database as:

y = c (+) *f (13)*

Furthermore, the secret s is hashed with a cryptographic hash function H and H(s) is stored in the database. This scheme is sketched in symbolical form in figure 3.

For authentication, the template *f**, presented by the user, is added to the value y stored in the database. The result is *f**(+) *y = f** (+) *c* (+) *f.* If the hamming distance between *f** and *f* is at most t, *c = G(s)* and hence s can be recovered. If the hash value of the recovered s matches the one stored in the database, the user is authenticated. This approach extracts a secret key from the biometric template presented and the corresponding public string. No information about this key shall be extractable from the public string without the corresponding biometric template.

Thus an error correction code must be device from the template and needs to be stored in a database. This code does not reveal any information about generating the template, rather can change the generated template such that the error with corresponding to the actual template from which the error correction code is derived is zero.
Thus we measure the bit error rate ratio as bit wise difference between the actual template and the generated template when the templates are converted into a binary bit stream. We adopt local binary patter generation technique for achieving the same.

2.6 Related Work

[1] Elaborates the various techniques for biometric data security by proposing a matching environment based on smart cards. It also elaborates the mechanism of generating a hash from the fingerprint biometric data and encrypting data through this hash.

Authors in [2] deal with the variability in the biometric templates. According to the finding of the author, every matching for authentication must also measure the quality of the just generated template and periodically must update the template in order to maintain high accuracy in biometric authentication process. The paper also presents matrices for biometric template quality analysis which is used in the proposed benchmark analysis work.

Authors in [3] elaborate the main problem with the conventional password based security techniques and emphasizes on the facts as to why the biometric keys are better than conventional keys. The work defines the technical steps associated with the keys and also discusses the properties of good biometric keys.

For biometric key generation from biometric features like faces and fingerprints, first image specific features must be extracted which is called templates. A quantization is applied on the template to generate the key. As real number range is infinity, if a key is generated without quantization, matching becomes a difficult process. Hence authors in [4] elaborate the mechanism for the quantization process for key generation. They also suggest a log likelyhood based technique for the same.

Even though biometric keys are strong technique for cryptographic key generation, because they are stored in the database, there remains a chance for the keys to be eavesdropped by unauthenticated users which makes the system vulnerable. Therefore techniques must also be adopted for such key generation. Hence authors in [5] proposes the techniques for securing the biometric key itself.

[6] proposes an Iris recognition technique with the help of bio orthogonal wavelets. But most importantly the authors in [6] proposes an encoding technique for the templates for ease in matching.

The strength of a biometric key is defined from the inability of a propoer guessing of a key using brute force technique. A biometric key appears random to any intruder. Therefore how he guesses the key depends upon the entropy information of a random variable that generates the key. [7] defines a mathematical relationship of probability of successful guess of a key with the entropy information of the templates and hence quantifies the fact that entropy analysis of any template is an important step in deciding the strength of the key.

The closeness of a template with the stored template depends upon the distance between the templates. This distance can be represented in various mathematical forms as proposed by the authors of [8]. The authors also proves experimentally that log likelyhood measure is one of the better way of representing the closeness of two templates.

Whenever a mechanism is selected for biometric template matching for authenticating purpose, it invariably presents a false rejection and false acceptance on the biometric data and the mechanism itself. The authors in [9] presents a unique way to select the appropriate tradeoff between the rejection and acceptance tradeoff so that the adopted technique is acceptable and efficient. The author also presents a benchmark analysis for optimality for any recognition technique in [10] and illustrate the proposed theory with the help of character recognition system. Gabor based techniques are widely adopted for biometric feature representation or generation of templates. But the size of such initial vectors is so high that it presents a practical problem of storage. Thus biometric template reduction becomes an important aspect for biometric key generation or authentication technique. [12] presents a technique for minimizing the number of feature vectors for template generation.

Out of all the possible attacks on biometric keys the most severe attack is on the stored keys. This findings of [13] forms a base for our assumption that if a system can be deviced without the necessatiy for the key to be saved, a biometric system can be made un-attackable. Even though the authors present multi biometric model for hardening the security of a biometric system, the system still remains vulnerable against the attacks.

For any biometric like face or fingerprints or iris, templates will differ from one instance to the other instance of acquisition. Therefore out of N number of aquistion of the templates of a single feature type of a person there would certainly exist a variability amongst the templates. Therefore authors in [14] presents a systematic way of extracting the best template out of all the templates. This paper also presents an important step for biometric feature benchmark analysis by proposing a clustering technique for seggegating the biometric features by their average distance measures.

As against most widely used gabor convolve methods, authors in [15] proves that biorthogonal wavelets achieve higher accuracy with low FAR and high FRR. Thus Biorthogonal wavelet based template generation is selected as one of the methods for testing the quality of a biometric template for experiments in this paper.

[16] classifies the type of attack on the stored biometric systems and proposes a unique mechanism for minimizing the risk emerging from such attack. But the authors presents an important finding that encrypting the biometric keys or appending more security layer for protecting the biometric data leads to more complicated processing in the recognition phase which delays the overall time for recognition. This findings also strengthens the need for a system which can empirically analyze the quality of a biometric system before adopting it.

[17] presents a technique to remove the need of a centralize storage for biometric data with the help of smart cards. But the authors also emphesis that even such a card based system cannot guarantee a perfect un attackable system as the user information can be eavesdropped from the card itself.

[18] discusses various techniques by means of which the biometric data itself (not the templates) can be acquired , forged and can be used. It also presents a wide verity of attacks and describes at which instance and which data sets the attacks can affect.

In [19] authors describes a technique for generation of digital signature from biometric template. Such signatures can be used in public key cryptography for encryption and decryption of digital documents shared across a network.

[20] analyzes the technique proposed by [11] to rectify the errors in generated template by using Reed Solmon code. The authors also proposes a unique mechanism for protection of biometric

key by storing the checksum rather than the key in the database. The authors also show that a key generation from biometric template and subsequent correction using the checksum improves the system security to a great deal. This work has adopted the elaborated model for error correction in biometric template.

In [21] authors have used irreversibility and revocability of the templates as a measurement for biometric key security and shows the technique of biometric matching in the secured environment. The authors present another significant observation here interms of feature selection. [21] finds that lower order features like means and standard deviation can not reveal the actual information of any feature set and higher order spectra is better suited for the representation of the features. Hence in our benchmark analysis, we have used a higher order spectra for determining the closeness of the templates.

[22] proposes an alternative method for biometric security through intronization. It is a process of adding extra feature systematically in the biometric template to increase the randomness of the template and also demonstrates that even after intronization, the achieved results are satisfactory.

[23] discusses one of the most least talked possible attacks on the biometric templates. The author here finds out a technique through which the image itself can be interpolated or reconstructed from leaked template. Therefore this image can be subsequently used to obtain un authorized information through hill climbing attack. Thus the findings demonstrates that not only the randomness of the templates are enough to provide security to the biometric system but at the same time it is also important to ensure that the inverse process of reconstruction of images should not be possible from the templates.

[24] elaborates a new technique called biometric template transformation be menas of which direct mathematical transformation can be achieved on the templates to extract more information from the templates. This important transformation is the answare for the following severe problem. Whenever a biometric key is encrypted, it can not be used for direct matching at the time of verification. The key needs to be decrypted before matching which invariably exposes the key. But with the help of direct transformation on the biometric templates, key matching can be performed over the encrypted keys, minimizing the requirement for a decryption stage prior to verification.

In [25] authors proves that presence of noise in the biometric data actually improves the security of the data itself. This claim is supported through entropy analysis of the generated key from the template and the relationship of energy and the entropy of the information.

[26] discusses various mathematical transformation related to guessing of a biometric key and presents a fish-bone model for categorization of the attacks on biometric data. The model helps in identifying various areas which must be considered for ensuring the security of biometric data.

[27] proposes a mechanism for mixing a biometric template with biometric key for biometric key protection.

[28] discusses about possible technique for face biometric and is used for selection of the techniques for the current work.

Merely ensuring a strong key generation technique is not sufficient for biometric technique adaptation. It must be checked for the feasibility of adaptation. [29] presents various means of feasibility check for biometric techniques.

[30] proposes an indexing scheme through binning to index the biometric images in a large database into groups for better classification and representation.

Authors in [31] discusses a unique technique for secured biometric mechanism by introduction of N-template system. The authors clasim and proves that if more than one template is generated from the same biometric feature like iris and a similarity measurement function can be deviced to find the similarity between the templates than, the empirical value of similarity can be used to authenticating the users rather than the template itself.

The method of selecting best templates or function that generates best templates are always result driven tests. Thus it is quite difficult to select the best templates out of available templates. [32] accesses this problem partially and presents a score based mechanism for template selection. In this work, the prototype of [32] is extended for selecting not only the best templates but for selecting the mechanism itself which can generate most acceptable templates.

[33] discusses various non technical issues alongside the technical issues for acception a biometric access control technique.

Improving the biometric recognition with 0% FAR and 0% FRR is considered to be ideal theoretical biometric system which is not yet achieved. Authors in [34] observe that most widely used technique for enhancing the security of a biometric system is through combining more than one modality like combining face and iris. But this needs the user to expose his features twice before two different sensors. Instead [34] proposes a mechanism to extract two different types of features from the same modality to enhance the recognition efficiency.

3. ALGORITHMIC APPROCH FOR BIOMETRIC TEMPLATE QUALITY BENCHMARK ANALYSIS

For analysis the quality of a specific biometric type and the template generated from the specific feature set of the template for time invariance analysis must be carried out with the following Model

i) First select d different type of biometric features like face, fingerprint, iris, Retina, Palm Print etc. We define D={Face,Iris,Fingerprint}---(14) as a set of different biometric types.

ii) U is a finite set of N users.

$$U = \{u_1, u_2, ..., uN_u\} \qquad (15)$$

iii) Select feature selection method for each type of D and let us consider that the feature

selection set is F

$$F = \{C_1, C_2, ..., C_{nc}, I_1, I_2, I_3, ..., I_{ni}, P_1, P_2, ...P_{np}\} \quad (16)$$

Where I,C,P represents feature selection methods for Iris, Face and Fingerprints respectively.

iv) Let T be a set of all the templates generated from all the feature selection technique from (14) with all the feature generation methods from (16) for all the users from (15).

$$T_i = \{T_{i1}, T_{i2}, T_{i3}, ..., T_{\mathrm{int}}\} \quad (17)$$

Where nt is total number of templates and are given by

$nt = nu \text{ x } ni \text{ x } np \text{ x } nc$ (18) and i is used to denote independent users.

$T = \{T_i\}$ where i=1,2,….nu (19)

Now let us consider that templates of separate instances of the same users are taken over the time and is represented by j.

Then (19) is redefined as

$T = \{T_{ij}\}$ (20) where j=1,2,3….t where t is the maximum number of instances.

The objective is to find best F for which

$T_{ij} EQ T_{i(j-1)}$

$T_{i(j-1)} EQ T_{i(j-2)}$

$T_{i(j-t)} EQ T_{i(j-t-1)}$ for all i (21)

(21) must also satisfy the constraints low SO and high SS as par equation (2) and (3).

Equal operator EQ is defined as the set of distance measurement techniques.

$EQ = \{D_1, D_2, D_3, ..., D_m\}$ (22)

Where m are different types of distance measurement.

From (18) it is clear that as number of users increases, total number of analysis step also increases. Therefore rather than checking for (21) after generating all the features we need to minimize the selected features such that total number of comparison does not increase with number of instances and user.

In order to process the number of processing in (21) we define following steps

a) Generate two instances of feature vectors from each user for every technique to form the set T_{ij} as in (20) for t=2.

b) For every user i, take the uncorrelated Euclidian distance E between template Ti1 and Ti2.

If(E_{ik}>95%) where k represents template generation method F from (16), then

Delete Fk.

Therefore at the end of step (b) F_1 will be a reduced length set of techniques nf2 where nf2<nf, the standard set of all techniques F of length nf. These are the techniques which produces most similar templates after two instance comparison.

c) Now divide the users into two categories C_1 the set of all genuine user and C_2 a set of all imposters. C_1 and C_2 are constructed randomly with any user having equal probability to be in the set C1 or C2.

Calculate average SSf and SOf with all templates from every independent Feature generation technique where suffix f represents a particular feature or template generation technique.

Find out average SSf and SOf as Assf and Asof.

Omit all the f for which following condition is false.

(SSf<Assf)&&(SOf>Asof).

Hence after step C, we obtain a new set of feature generation technique F3 where nf3 or the length of feature selection technique is less than nf_2.

d) Now construct independent set I_3,C_3 and P_3 as set of techniques generating Iris features, face features and fingerprint features respectively.

Let the new length of the sets be $n_{i3}, n_{c3},$ and n_{p3} respectively.

Select the Biometric feature set B as the maximum of $n_{i3}, n_{c3},$ and n_{p3}.

Hence $B = \max(n_{i3}, n_{c3}, n_{p3})$ € D (23).

Omit all F3 other than those belonging to B.
Thus finally F4 is the set of a feature generation techniques with High SO and low SS of either face or fingerprint or Iris.

e) Regenerate Template set T_{ij} as in (20) for t=2. Now T_{ij} must be further optimized to find out the techniques which satisfies the posterior probability principal calculated as (7) through (8) (9) and (10).

f) Finally after step e) we have all the template generation techniques which presents high autocorrelation with same class, low self similarity, high other similarity and high posterior probability. Thus the biometric key generated using these set of methods are better suited for proposed method as in finger 2.

g) Finally a bit stream is generated by using local binary patterns and the error correction code is saved as in section 2.5

h) Equation (20) is now checked by considering t where t>>2. Here Operator EQ is defined as the hamming distance between current Binary template and the previous binary template. At this step we can select the technique or set of techniques which are best suited to generate most time invariant templates.

4. TESTING AND RESULTS

For Face database, Yale face database B is used which contains 5760 single light source images of 10 subjects each seen under 576 viewing conditions (9 poses x 64 illumination conditions). For every subject in a particular pose, an image with ambient (background) illumination was also captured.

The IIT Delhi Iris Database is used for testing the iris images. The currently available database is from 224 users, all the images are in bitmap (*.bmp) format. All the subjects in the database are in the age group 14-55 years comprising of 176 males and 48 females. The database of 1120 images is organized into 224 different folders each associated with the integer identification/number. The resolution of these images is 320 x 240 pixels and all these images were acquired in the indoor environment.

FVC2004 Fingerprint database with DB1 and DB2 with both seta and setB are considered for testing the algorithms on the fingerprint images. Each database is 150 fingers wide and 12 samples per finger in depth i.e., it consists of 1800 fingerprint images.
Result Tables are developed by aggregating the results of images from independent classes.

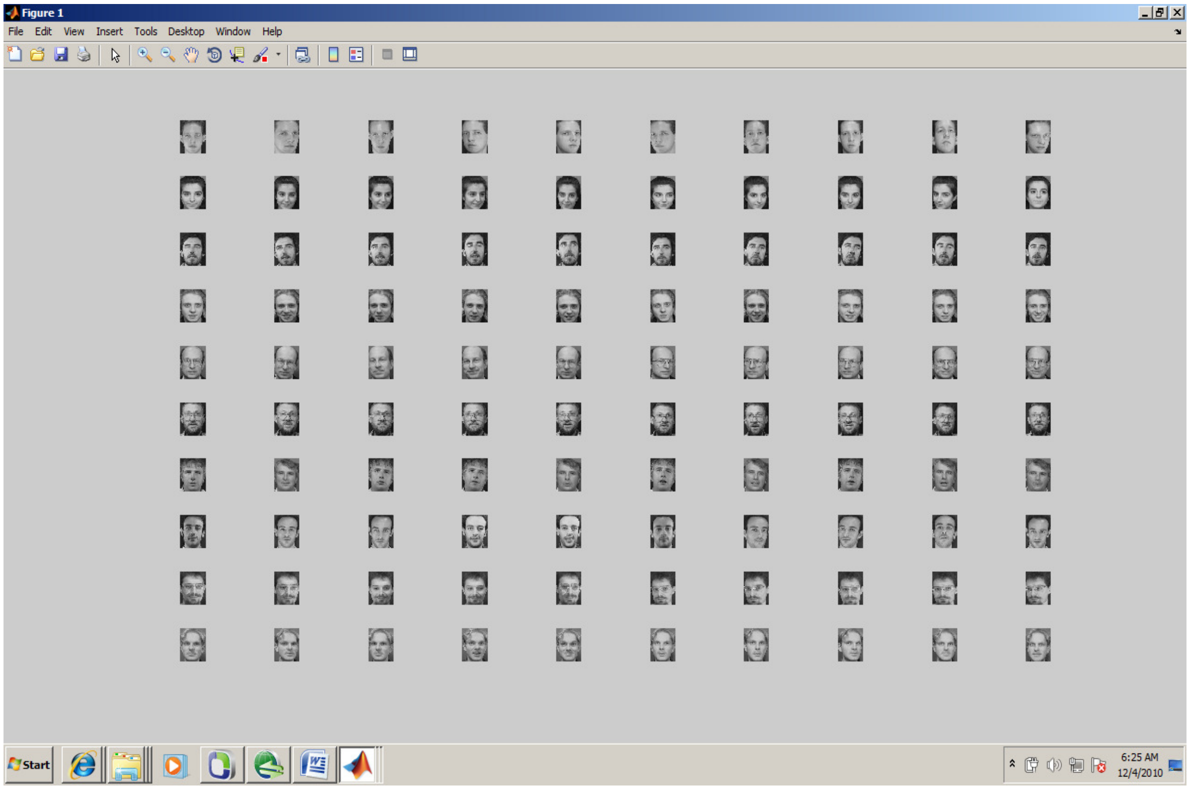

FIGURE 4: Face Database

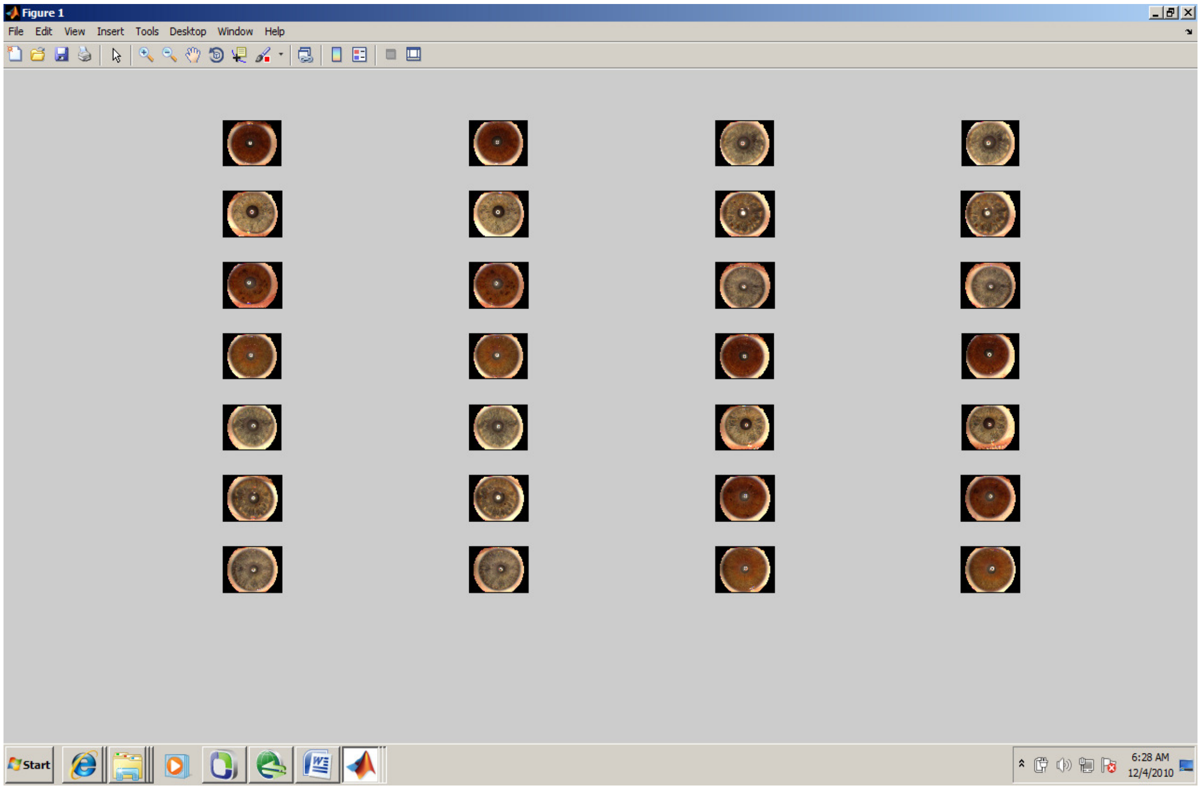

FIGURE 5: IRIS database

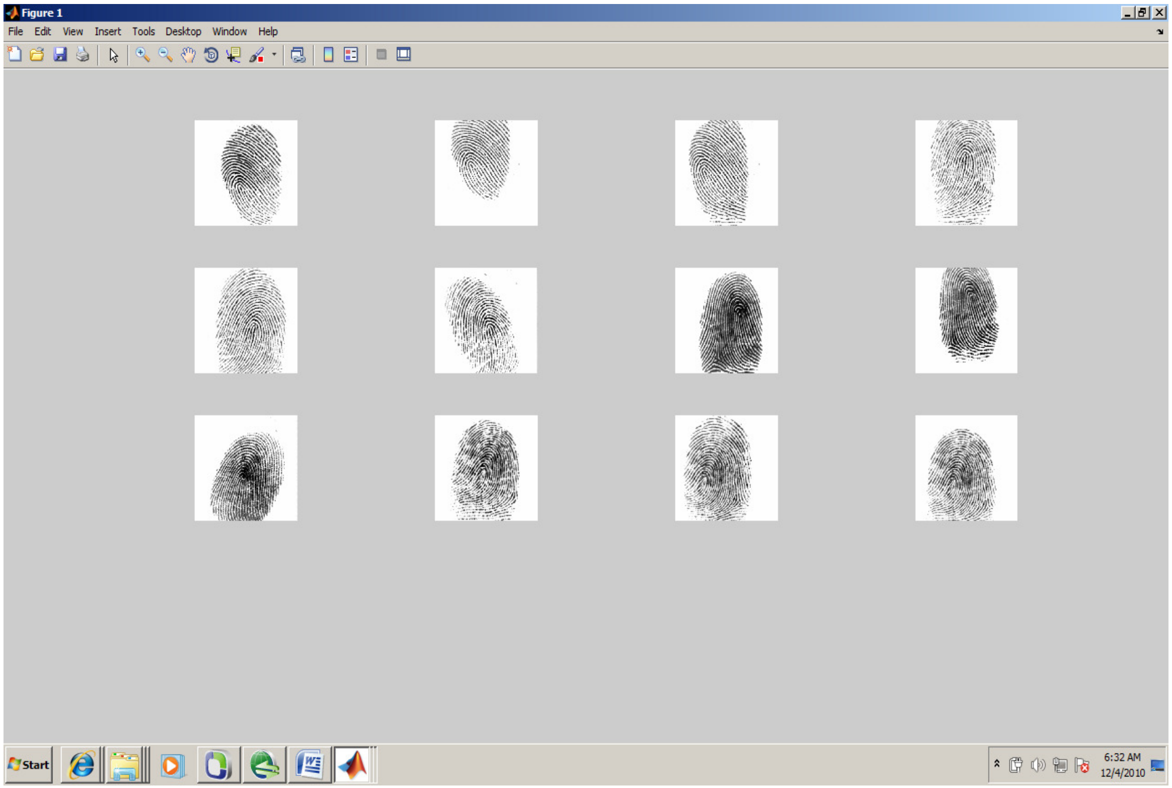

FIGURE 6 : Fingerprint Database

Method	Hx	Gd	Average Ed	SS	SO	BER
GLCM	.12	11.63	1.03	1e-3	5291.35	.2e-11
Wavelet	.471	21.57	1.11	.7e-3	588.334	16e-11
Gabor Convolve	.14	29.519	.0071	.3e-4	2181.0	1.9e-19
PCA	.11	29.6	.031	.000132	2664.1	1e-20
ICA	.663	13.64	4.34	.0096	998.03	1e-8
BEST	PCA	GABOR/PCA	GABOR	GABOR	PCA	PCA

TABLE 1: Sample Face Statistics Summery

Method	Hx	Gd	Average Ed	SS	SO	BER
GLCM	.29	1.761	2.17	.009	471.55	1e-9
Wavelet	.27	4.17	9.11	.003	426.334	1e-10
Gabor Convolve	.22	19.0085	3.21	.0001	1781.76	1e-19
PCA	.19	16.6	1.61	.00087	1864.122	1e-19
ICA	.263	.64	7.64	.056	1011.03	1e-14
BEST	PCA	GABOR	PCA	GABOR	PCA	PCA/GABOR

TABLE 2: Sample summery of Fingerprint based methods

Method	Hx	Gd	Average Ed	SS	SO	BER
GLCM	.45	.0761	12.33	.049	176.55	1e-8
Wavelet	.21	.0017	6.34	.003	526.14	1e-12
Gabor Convolve	.12	.00083	2.21	.0001	1271.76	1e-13
PCA	.16	.0016	4.61	.00027	1464.882	1e-17
ICA	.31	.064	8.64	.051	1011.03	1e-14
BEST	GABOR	GABOR	GABOR	GABOR	PCA	PCA

TABLE 3: Summary of performance of IRIS biometric templates

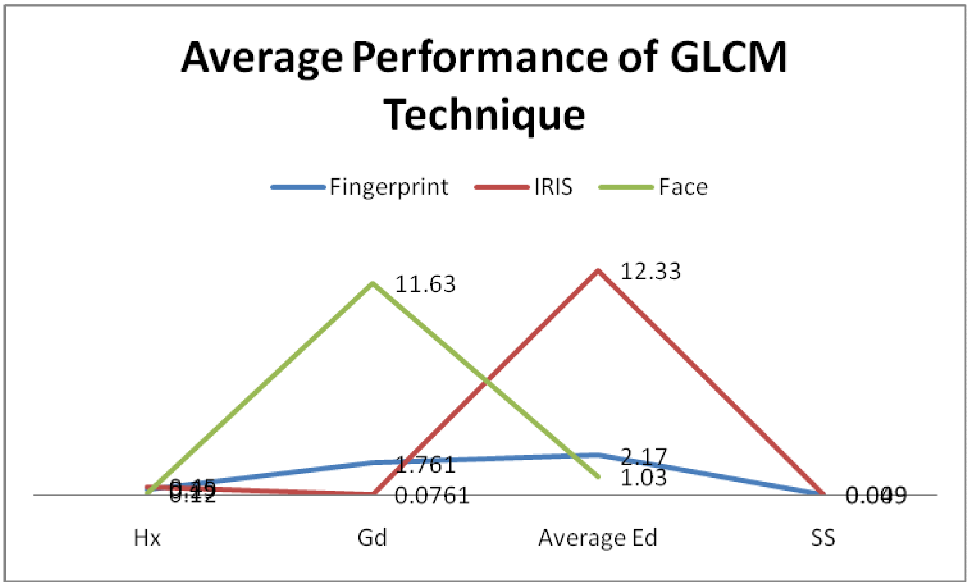

FIGURE 7: Avergare Performance of The GLCm technique

It is clear from Figure 7 that GLCM is a suitable technique for IRIS and Fingerprint due to low SS,HX and High GD. Though for face recognition system presents a very high Ed which makes it not a good choice for Face Recognition.

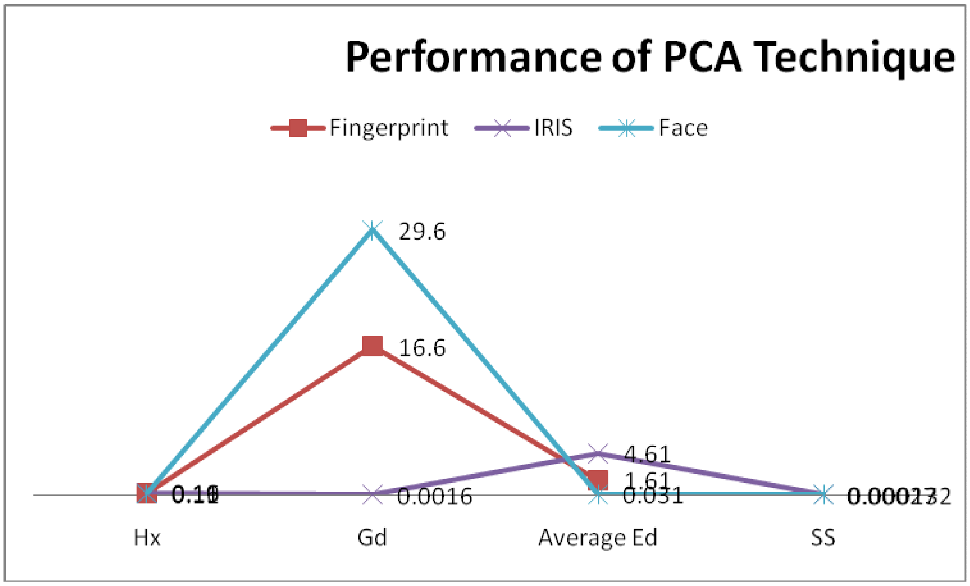

FIGURE 8: Performance of PCA with respect to all the techniques

The result demonstrate that PCA for classification of face , IRI and Fingerprint provides the desired properties of low Hx, High Gd, low SS and Hence can be adopted as universial biometric feature for any of the three biometrics with optimum result.

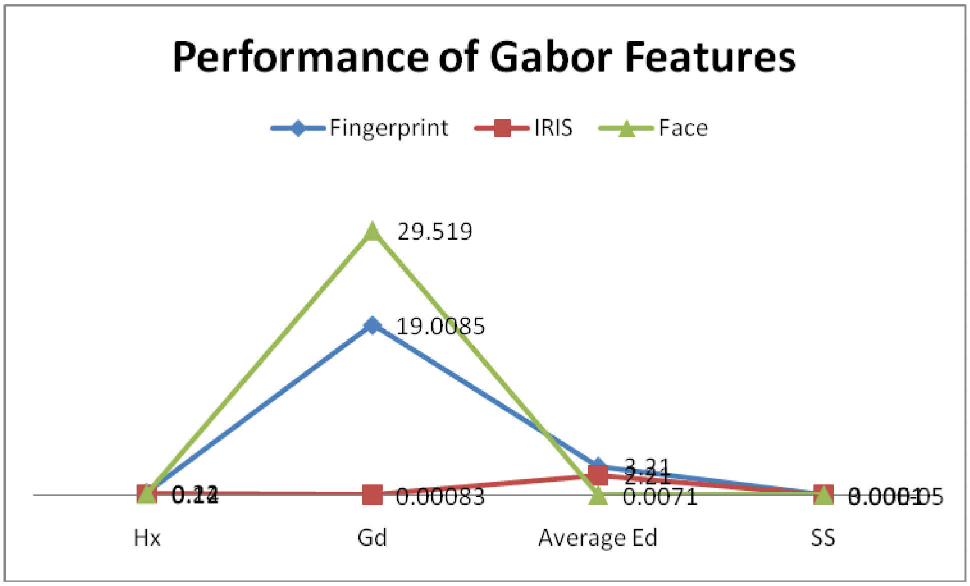

FIGURE 9: Performance of Gabor features for various biometrics also shows desireable result for all the biometrics.

In comparision to other techniques, Gabor convolve features and PCA features are more universially suitable for biometric recognition.

Hence it can be claimed that both of these features are more invariable and are more suited to biometric recognition.

5. CONCLUSION

Selecting an appropriate biometric model is an important step towards achieving high performance solutions. A lot of factors like scalability, usability and invariability must be analyzed amongst the models and the feature selection type for the template before finalizing the selection. Many work is proposed towards improving the efficiency of particular biometric technique as reviewed in related work. But there has not been any standard benchmark which offers a systematic analysis of benchmark of the performance of the system. In this work an entirely new approach of benchmark analysis for the quality of the selected biometric model and the technique is proposed based on invariability analysis of the templates from instance to instance. Results shows that IRIS has better invariability from both face and fingerprints and also offers better SO and SS values desired for high accuracy classification. The result also suggests that once time and instance invariant templates are generated, binarization process will always contain least bit error. Hence before any biometric model and technique is adopted, if the techniques available for the models are analyzed using this method, it can give an assurance of performance over the use. Further the proposed technique can be tested with many different other algorithms developed over the years for all the considered biometric model to present the proof of acceptance.

3. REFERENCES

[1] Magnus Pettersson, “The Match On Card Technology”, *Precise Biometrics White Paper*

[2] Ricardo García Noval, Francisco Perales López, “Poster: Adaptative Templates In Biometric Authentication”

[3] Lucas Ballard, Seny Kamara, Michael K. Reiter, “The Practical Subtleties of Biometric Key Generation”, *17th USENIX Security Symposium*

[4] C. Chen, R.N.J. Veldhuis, T.A.M. Kevenaar, A.H.M. Akkermans, “Multi-Bits Biometric String Generation based on the Likelihood Ratio”, *DOI: Multi-Bits Biometric String Generation based on the Likelihood Ratio,IEEE, 2007*

[5] U. Korte, R. Plaga, “Cryptographic Protection of Biometric Templates: Chance, Challenges and Applications”

[6] Aditya Abhyankar , Stephanie Schuckers, “Novel Biorthogonal Wavelet based Iris Recognition for Robust Biometric System”, *International Journal of Computer Theory and Engineering, Vol. 2, No. 2 April, 2010 1793-8201*

[7] James L. Maseey, “Guessing and Entropy”,*DOI: 0 - 7803-2015-8/94, IEEE,1994*

[8] Asker M. Bazen and Raymond N. J. Veldhuis, “Likelihood-Ratio-Based Biometric Verification”, *Ieee Transactions On Circuits And Systems For Video Technology, Vol. 14, No. 1, January 2004, 1051-8215/04,Ieee, 2004*

[9] C. K. CHOW, “On Optimum Recognition Error and Reject Tradeoff”, *IEEE Tr.4nsactions On Information Theory, Vol. It-16, No. 1, January 1970*

[10] C. K. CHOW, “An Optimum Character Recognition System Using Decision Functions”, *PGEC, June 3, 1957*

[11] Juels A. and Wattenberg M., "A Fuzzy Commitment Scheme", ACM Conference on Computer and Communications Security", 1999, p.28-36

[12] Daniel Gonz´alez-Jim´enez and Jos´e Luis Alba-Castro, "Modeling Marginal Distributions of Gabor Coefficients: Application to Biometric TemplateReduction", *project PRESA TEC2005-07212*

[13] V. S. Meenakshi and Dr G. Padmavathi, "Securing Revocable Iris and Retinal Templates using Combined User and Soft Biometric based Password Hardened Multimodal Fuzzy Vault", *IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 5, September 2010 ISSN (Online): 1694-0814*

[14] Anil Jain, Umut Uludag and Arun Ross, "Biometric Template Selection: A Case Study in Fingerprints", *Proc. of 4th Int'l Conference on Audio- and Video-Based Person Authentication (AVBPA), LNCS 2688, pp. 335-342, Guildford, UK, June 9-11, 2003.*

[15] Aditya Abhyankar and Stephanie Schuckers, "Novel Biorthogonal Wavelet based Iris Recognition for Robust Biometric System", *International Journal of Computer Theory and Engineering, Vol. 2, No. 2 April, 2010 1793-8201*

[16] Abhishek Nagar, Karthik Nandakumar, and A. K. Jain, "Biometric template security", *SPIE, 10.1117/2.1200911.001590*

[17] Julien Bringer, Herve Chabanne, David Pointcheval, and Sebastien Zimmer, "An Application of the Boneh and Shacham Group Signature Scheme to Biometric Authentication", *Springer-Verlag 2008*

[18] Qinghan Xiao, "Security Issues in Biometric Authentication", *Proceedings of the 2005 IEEE,Workshop on Information Assurance and Security, United States Military Academy, West Point, NY*

[19] Yunsu Chung, Kiyoung Moon, Hyung-Woo Lee, "Biometric Certificate based Biometric Digital Key Generation with Protection Mechanism", *Frontiers in the Convergence of Bioscience and Information Technologies 2007*

[20] Andrew Beng Jin Teoh, Thian Song Ong, "Secure Biometric Template Protection via Randomized Dynamic Quantization Transformation", *1-4244-2427-6/08,IEEE*

[21] Brenden Chen and Vinod Chandran, "Biometric Template Security Using Higher Order Spectra", *978-1-4244-4296-6/10, IEEE,2010*

[22] Qinghai Gao, Xiaowen Zhang, and Michael Anshel, "Experiments on Matching Intronized Fingerprint Minutiae Templates", *IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.9, September 2008*

[23] Andy Adler, "Vulnerabilities in biometric encryption systems", *IST-044-RWS-007*

[24] Michael Braithwaite, Ulf Cahn von Seelen, James Cambier,, "Application-Specific Biometric Templates"

[25] E. Verbitskey,D. Denteneer, P. tuylys, "Reliable biometric authentication with privacy protection."

[26] Anil K. Jain, Karthik Nandakumar, and Abhishek Nagar, "Biometric Template Security", *EURASIP Journal on Advances in Signal Processing Volume 2008, Article ID 579416, 17 pages, doi:10.1155/2008/579416*

[27] Shih-Wei Sun¤*y*, Chun-Shien Lu¤, and Pao-Chi Chang*y,* “Biometric Template Protection: A Key-Mixed Template Approach”, *1-4244-0763-X/07, IEEE, 2007*

[28] Morpho, “Automatic Facial Recognition: A review”, *SAFRON*

[29] Tony Mansfield, Marek R. G., “Feasibility study on the use of biometric in an Entitlement scheme, Biometric Feasibility Study”, *Version 3, 2003*

[30] Srinivasa Palla, Sharat S. Chikkerur, Venu Govindaraju, Pavan Rudravaram, “Classification and Indexing in Large Biometric Databases”

[31] Tarachand Verma, Prof. Richa Jindal, Prof. Sonika Jindal, “A Security Algorithm For Iris Based Biometric System”, *International Journal Of Engineering Science And Technology, Vol. 2(06), 2010, 2316-2320*

[32] Yong Li, Jianping Yin, En Zhu, Chunfeng Hu, Hui Chen, “Score Based Biometric Template Selection”, *978-1-4244-2175-6/08/, IEEE, 2008*

[33] Luisa Riccardi, Bruno Peticone and Mario Savastano, “Biometrics for massive access control Traditional Problems and Innovative Approaches”, *Proceedings of the 2005 IEEE Workshop on Information Assurance and Security United States Military Academy, West Point, NY*

[34] C.Lakshmi Deepika, A.Kandaswamy, “An Algorithm for Improved Accuracy in Unimodal Biometric Systems through Fusion of Multiple Feature Sets”, *ICGST-GVIP Journal, ISSN 1687-398X, Volume (9), Issue (III), June 2009*