International Journal of Engineering Science Invention
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org Volume 3 Issue 11. 2014 ǁ PP.14-24

Chaos based Cancellable Biometric Template Protection Scheme-A Proposal

Supriya V G[1], S Dr Ramachandra Manjunatha[2]
[1]Research Scholar, Jain University, Bangalore, 560004, India
[2]Professor, Jain University, Bangalore, 560004, India

ABSTRACT *:* *Security of Information and ensuring personal privacy are growing concerns in today's society. Most concerns against the common use of biometrics arise from the storage and misuse of biometric data. In present scenario, Biometric cryptosystems and Cancelable biometrics are the two emerging technologies to address these concerns in order to improve public confidence. In the past ten years a significant amount of approaches to both technologies have been published. In this paper, a detailed survey of biometric cryptosystems and cancelable biometrics along with the open issues and challenges are discussed. A new approach based on cancellable biometrics using chaotic maps which are known to posses desirable properties of pseudo randomness, high sensitivity to initial conditions and very large key space is proposed to address these open issues and challenges.*

KEYWORDS - *Biometrics, Biometric Cryptosystems, Cancelable Biometrics, Chaotic maps.*

I. INTRODUCTION

Biometrics refers to the automatic identification (or verification) of an individual (or a claimed identity) by using certain physical or behavioral traits associated with the person viz. fingerprints, hand geometry, iris, retina, face, vasculature patterns, signature, gait, palm print, or voice print. Recently, since computer speed, media storage and network bandwidth have seen great improvements of their performances, biometric systems has gained even more importance along with security, privacy and intellectual property defense, recent one being its usage in the Aadhar card or the Unique Identification card for the citizens of India. Although the convenience of a biometric system is increasing, the biometric template protection becomes more and more important. Most of the biometric systems store the extracted biometric template in a centralized database for authentication applications. Since biometric characteristics are permanently associated with user, a compromise of biometric templates results in permanent loss of a subject's biometrics. Standard encryption algorithms compare biometric templates in decrypted domain and leave biometric templates exposed during every authentication attempt [2] which are vulnerable to attacks and can decline its security. Ratha et al [9] analyzed these attacks and grouped them into eight classes. Concept of Cancellable Biometrics is one of the original solutions to address these concerns in which instead of storing original biometric, the biometric is transformed using a one-way function. This preserves privacy since it is computationally very hard to re-cover the original biometric from a transformed version. Biometric template protection schemes are commonly categorized as Biometric Cryptosystems referred as helper data-based schemes and Cancelable Biometrics referred as feature transformation which are designed to meet two major requirements of biometric information protection [1].

- Irreversibility: It should be computationally hard to determine any information about the original biometric template from the stored reference data, while it should be easy to generate the protected biometric template.
- Unlinkability: The unique biometric data (renewability) can be used to generate different versions of protected biometric templates, while not allowing their cross-matching (diversity).

"Biometric Cryptosystems (BCSs) are designed to securely bind a digital key to a biometric or generate a digital key from a biometric" [6]. BCSs offer solutions to biometric-dependent key-release and biometric template protection [10]. It replaces the password-based key-release and brings about substantial security benefits. It is significantly more difficult to forge, copy, share and distribute biometrics compared to passwords [1]. BCSs are designed to output stable keys which are required to match a 100% at authentication. Original biometric templates are replaced by biometric-dependent public information which assists the key-release process.

"Cancelable Biometrics (CB) consists of intentional, systematically repeatable distortions of biometric signals based on transforms which provide a comparison of biometric templates in the transformed domain" [9]. Biometrics cannot be revoked when spoofed. Therefore, instead of storing the biometrics, transformed templates are stored. The inversion of such transformed biometric templates must not be feasible for potential imposters. In contrast to templates protected by standard encryption algorithms, transformed templates are never decrypted since the comparison of biometric templates is performed in transformed space which is the very essence of CB. The application of transforms provides irreversibility and unlinkability of biometric templates [6], which prevents the use of same captured template for other applications.

In this paper, systematic classification and in depth discussion of approaches to BCS and CB Systems are discussed in detail. The open issues and challenges concerned to BCS and CB Systems are listed and discussed. To address some of these issues and challenges, we proposed a new method for biometric template protection based on chaotic functions. The very high key sensitivity and large key space properties of chaotic stream ciphers are useful in addressing problems in BCS and CB Systems.

Chaos theory is a field of study in mathematics discovered by Edward Lorenz. Chaos theory studies the behavior of dynamical systems that are highly sensitive to initial conditions. Its response is popularly referred to as the butterfly effect. Chaos is a deterministic and random-like process. Because of its random-like behavior, sensitivity to initial conditions & parameter values and confusion & diffusion properties, chaotic cryptography has become an important branch of modern cryptography. Small differences in initial conditions yield extensively diverging outcomes for such dynamical systems, rendering long-term prediction impossible in general.

The properties of chaotic systems are:

- Deterministic i.e. they have some determining mathematical equations controlling their behavior.
- Unpredictable and non-linear i.e. they are highly sensitive to initial conditions. Even a very slight change in the starting point can lead to entirely different outcomes.

They appear to be random and disorderly but in actual they are not. Beneath the random behavior there is a sense of order and pattern. The highly unpredictable and random nature of chaotic output is the most attractive feature of deterministic chaotic system that makes it suitable to use in image transformation techniques.

Logistic Map is a one-dimensional chaotic map proposed by R.M.May [78]. It represents an idealized conservation model for describing yearly variation in the population of an insect specie. The population at (n+1)th year is related to that at the (n)th year by the following mathematical equation:

$$x_{n+1} = r * x_n[1 + x_n] \qquad 0 < x < 1 \qquad (1)$$

Here x_n represents the chaotic sequence which lies between zero and one. When the system parameter r is varied over the interval [0,4] different scenarios of evolutionary behavior are established. The iterates are confined to [0,1]. Depending on the value of r equation (1) has got several properties. With r between 0 and 1, the population will eventually die, independent of the initial population xn. When r is between 3 and 3.45 the value of x_n will oscillate between two values. With slightly bigger r values the value of x_n will oscillate between 4 values, then 8,16,32 etc. Like a period doubling cascade. When the value of r is 3.57 it will start exhibiting chaotic behavior.

The rest of this paper is organized as follows: In Section 2 and 3, BCS and CB systems are categorized and concerning literature is reviewed in detail. Security risks, privacy aspects, open issues and challenges are presented in section 4. In section 5, a novel chaos based cancellable biometric template protection scheme is proposed. In section 6, the performances of the proposed scheme is analysed and discussed to address the listed challenges. Finally, conclusions are given in Section 7.

2. Biometric cryptosystems

The majority of BCSs require the storage of biometric-dependent public information, which is applied to retrieve or generate keys, also referred to as helper data [2]. Helper data must not reveal significant information about original biometric templates, which assists in reconstructing keys. Biometric comparisons are performed indirectly by verifying key validities, where the output of an authentication process is either a key or a failure message. Based on how helper data are derived, BCSs are classified as key-binding and key-generation systems.

2.1 Key-binding schemes

In this scheme helper data are obtained by binding a chosen key to a biometric template. By applying an appropriate key retrieval algorithm, keys are obtained from the helper data at authentication [5].

In 1999 Juels and Wattenberg [11], techniques from the area of error correcting codes and cryptography are combined to achieve a new type of cryptographic primitive. This cryptographic primitive is referred to as Fuzzy Commitment Scheme. Rathgeb and Uhl [13] provide a systematic approach to the construction of Iris-based Fuzzy Commitment Schemes. After analyzing the error distributions between the iris-codes of different iris recognition algorithms, Reed-Solomon and Hardamard codes are applied. In [14] the authors apply context-based reliable component selection in order to extract keys from iris-codes, which are then bound to Hadamard codewords. Different techniques to improve the performance of Iiris-based Fuzzy Commitment Schemes have been proposed in [15-17]. Nandakumar [20] applies a binary fixed-length minutiae representation, obtained by quantizing the Fourier phase spectrum of a minutia set in a fuzzy commitment scheme, where alignment is achieved through focal point of high curvature regions. A method based on user adaptive error correction codes proposed by Maiorana et al. [21] adaptively selects the error correction information based on the intra-variability of a user's biometric data. Applying online signatures seems to be the first approach of using behavioral biometrics in a fuzzy commitment scheme. In [22] another fuzzy commitment scheme based on online signatures is presented. The first practical and most apparent implementation of the fuzzy vault scheme proposed by Clancy et al. [24], locks minutiae points in a "fingerprint vault". A set of minutiae points, A, are mapped onto a polynom p and chaff points are randomly added to construct the vault. Reed-Solomon codes are applied to reconstruct the polynom p, out of which a 128-bit key is recreated during authentication. A pre-alignment of fingerprints is assumed where feature alignment represents a fundamental step in conventional fingerprint recognition systems. To overcome the assumption of pre-alignment, Nandakumar et al. [25] suggest to utilize high curvature points derived from the orientation field of a fingerprint as helper data to assist the process of alignment. In their fingerprint fuzzy vault, 128-bit keys are bound and retrieved. Moon et al. [26] suggest to use an adaptive degree of the polynomial. Nagar and Chaudhury [27] arrange encoded keys and biometric data of fingerprints in the same order in separate grids, which form the vault. Chaff values are inserted into these grids in appropriate range to hide information. Additionally, the authors propose another syndrome-based key-generating scheme which they refer to as PinSketch. This scheme is based on polynomial interpolation like the fuzzy vault, but requires less storage space. Arakala [29] provides an implementation of the PinSketch scheme based on fingerprints. Kumar and Kumar [30,31] present a fuzzy vault based on palmprints by employing real-valued DCT coefficients of palmprint images binding and retrieving 307 bit keys.

2.2 Key-generation schemes

In this scheme helper data are derived only from the biometric template. Keys are directly generated from the helper data and a given biometric sample [2]. A technique applied to face biometrics called "BioHashing" was introduced by Teoh et al. [18,32-33]. Basically, the BioHashing approach operates as key-binding scheme, however, to generate biometric hashes secret user-specific tokens have to be presented at authentication. Prior to the key-binding step, secret tokens are blended with biometric data to derive a distorted biometric template, thus, BioHashing can be seen as an instance of "Biometric Salting".

Kong et al. [34] presented an implementation of Face Hashing and gave an explanation for the zero EER, reported in the first works on BioHashing. Zero EER were achieved due to the tokenized random numbers, which were assumed to be unique across subjects. Teoh et al. [35] address the so-called "stolen-token" issue evaluating a variant of BioHashing, known as Multistage Random Projection (MRP). By applying a multi-state discretization the feature element space is divided into 2N segments by adjusting the user-dependent standard deviation. By using this method, elements of the extracted feature vector can render multiple bits instead of 1 bit in the original BioHash. As a result, the extracted bit streams exhibit higher entropy and recognition performance is increased even if impostors are in possession of valid tokens. However, zero EERs were not achieved under the stolen-token scenario. Different improvements to the BioHashing algorithm have been suggested [36,37].

Nandakumar and Jain [38] proposed the best performing multibiometric cryptosystem in a fuzzy vault based on fingerprint and iris. It is confirmed that a combination of biometric modalities leads to increased accuracy and higher security. A FRR of 1.8% at a FAR of ~0.01% is obtained, while the corresponding FRR values of the iris and fingerprint fuzzy vaults are 12 and 21.2%, respectively. Numerous ideas of using a set of multiple biometric characteristics within BCSs have been proposed [40-44].

Nagar et al. [12,28] proposed a hybrid fingerprint-based BCS. Local minutiae descriptors, which comprise ridge orientations and frequency information, are bound to ordinate values of a fuzzy vault applying a fuzzy commitment scheme. In experiments FRR of 5% and a FAR of 0.01% is obtained, without minutiae descriptors the FAR increased to 0.7%. A similar scheme has been suggested in [45]. Chen et al. [46] extract keys from fingerprints and bind these to coefficients of n-variant linear equations. Any n ($n < m$) elements of an m-dimensional feature vector can retrieve a hidden key where the template consists of true data, the solution space of the equation, and chaff data (false solutions of the equation). A FRR of 7.2% and zero FAR are reported. Bui et al. [47] propose a key-binding scheme based on face applying quantization index modulation which is originally targeted for watermarking applications.

III. CANCELLABLE BIOMETRICS

Cancelable biometric transforms are designed in a way that it should be computationally hard to recover the original biometric data. The intrinsic strength (individuality) of biometric characteristics should not be reduced applying transforms (constraint on FAR) while on the other hand transforms should be tolerant to intra-class variation (constraint on FRR) [9]. In addition, correlation of several transformed templates must not reveal any information about the original biometrics (unlinkability). Two main categories of CB are distinguished [2].

3.1 Non-invertible transforms

In this approach, biometric data is transformed by applying a noninvertible function. The advantage of applying non-invertible transforms is that potential impostors are not able to reconstruct the entire biometric data even if transforms are compromised. Whereas applying non-invertible transforms may cause loss of accuracy. Difficulty in aligning the transformed biometric templates to perform a comparison has caused reduced performance and in addition information is also reduced. These effects have been observed for various approaches [9,51].

3.2 Invertible transform or Biometric salting

Biometric salting usually denotes transforms of biometric templates which are selected to be invertible. In any invertible transform of biometric feature, vector elements represents an approach to biometric salting even if biometric templates have been extracted in a way that it is not feasible to reconstruct the original biometric signal [52]. Finally, the parameters of the transform have to be kept secret. In case user-specific transforms are applied, the parameters of the transform, which can be seen as a secret seed [35] have to be presented at each authentication. If underlying biometric algorithms do not provide high accuracy with secret transforms, compromised transform parameters will enable Impostors to recover the original biometric template, causing a potential performance decrease of the system. While approaches to biometric salting may maintain the recognition performance of biometric systems, non-invertible transforms provide higher security [2].

In this technique, the authors first extract the most discriminative projections of the face template using fisher discriminant analysis [17] and then project the obtained vectors on a randomly selected set of orthogonal directions. This random projection defines the mechanism for the scheme called salting. Ratha et al. [9] were the first to introduce the concept of CB applying noninvertible transforms. During enrollment, non-invertible transforms are applied to biometric inputs by selecting application-dependent parameters. Whereas at the time of authentication, biometric inputs are transformed and a comparison of transformed templates is performed.

Boult et al. [58,59] proposed cryptographically secure biotokens which they applied to face and fingerprints. In order to enhance security in biometric systems, biotokens, which they refer to as Biotope, are adopted to existing recognition schemes.

Savvides et al. [52] generate cancelable face biometrics by applying so-called minimum average correlation filters which provide non-invertibility. User-specific secret personal identification numbers (PINs) serve as seed for a random basis for the filters. Ouda et al. [60,61] propose a technique to obtain cancelable iris-codes. i.e. Key dependent feature extract a vector of consistent bits (Bio Code) and their respective positions from several enrollment templates. Revocability is provided by encoding the BioCode according to a selected random seed. Pillai et al. [62] achieve cancelable iris templates by applying sector random projection to iris images. Recognition performance is only maintained if user-specific random matrices are applied.

Yang et al. [63] apply random projections to minutiae quadruples to obtain cancelable fingerprint templates. In further work [64] the authors address the stolen-token scenario by selecting random projection matrices based on biometric features. Hirata and Takahashi [65] propose CB for finger-vain patterns where images are transformed applying a Fourier-like transform. The result is then multiplied with a random filter where the client stores the inverse filter on some token. At authentication the inverse filter is applied to regenerate the transformed enrollment data and correlation-based comparison is performed. A similar scheme is applied to fingerprints in [66]. Bringer et al. [67] presented an idea of generating time-dependent CB to achieve untraceability among different identities across time. Several types of transforms for constructing multiple CB from pre-aligned fingerprints and face biometrics have been introduced in [9,54] including cartesian transform and functional transform. In further work [51], different techniques to create cancelable iris biometrics have been proposed. The authors suggest four different transforms applied in image and feature domain where only small performance drops are reported. Hammerle-Uhl et al. [53] applied classic transformations suggested in [9] to iris biometrics. Furthermore, in [55] it is shown that applying both transforms to rectangular iris images, prior to preprocessing, does not work. Similar to [51] Rathgeb and Uhl [56] suggest to apply row permutations to iris-codes. Maiorana et al. [57] apply non-invertible transforms to obtain cancelable templates from online signatures. In their approach, biometric templates, which represent a set of temporal sequences, are split into non-overlapping sequences of signature features according to a random vector which provides revocability. Subsequently, the transformed template is generated through linear convolution of sequences. The complexity of reconstructing the original data from the transformed template is computationally as hard as random guessing.

IV. SECURITY ISSUES AND CHALLENGES OF BIOMETRIC CRYPTOSYSTEMS AND CANCELABLE BIOMETRICS

To prevent biometric keys from being guessed, it is necessary to exhibit sufficient size and entropy. BCS performance is generally reported in terms of FRR and FAR, since both metrics and key entropy depend on the tolerance levels allowed at comparison, these three quantities are highly inter-related. Buhan et al. [23,48] have shown direct relation between the maximum length k of cryptographic keys and the error rates of the biometric system as $k \leq -\log2(FAR)$, which has established as one of the most common matrices used to estimate the entropy of biometric keys. Obviously, key lengths have to be maximized in order to minimize the guessing of secret keys [49].

The other factor which affects the security of biometric cryptosystems is privacy leakage, i.e., the information that the helper data contain about biometric data [50]. Ideally, for a given key length biometric security systems should not leak any information regarding helper data to avoid identity fraud. The requirements on key size and privacy leakage define a fundamental trade-off within approaches to BCS, which is not addressed.

While in majority of approaches, security is put on a level with obtained recognition accuracy, analysis with respect to irreversibility and unlinkability is not addressed. According to irreversibility, applied feature transformations have to be analyzed in detail.

In order to provide renewability of protected biometric templates, applied feature transformations are performed based on distinct parameters, i.e., employed parameters define a finite key space. In general, protected templates differ more as the respective transformation parameters are more distant [57]. To satisfy the property of unlinkability, different transformed templates, generated from a single biometric template applying different parameters, have to appear random to themselves.

Even though, with respect to the design goals, BCS and CB systems provides significant advantages to enhance the privacy and security of biometric systems, several new issues and challenges which arise deploying these technologies [7,1] are listed below.

- One fundamental challenge, regarding both technologies, represents the issue of alignment, which significantly effects recognition performance.
- To satisfy the property of unlinkability, different transformed templates, generated from a single biometric template applying different parameters, have to appear random to themselves.
- To prevent biometric keys from being guessed, these need to exhibit sufficient size and entropy.

In this paper, a novel chaos based cancellable biometric template protection scheme using Chaotic Signals is proposed to address the above challenges. The chaotic maps give excellent pseudorandom sequences [64] and very simple operations as compared to conventional transformation algorithm like AES [69] which involves large number of operations and consumes more time for transformation.

V. PROPOSED CANCELLABLE BIOMETRIC TEMPLATE PROTECTION SCHEME BASED ON CHAOTIC MAPS

In this section, a novel chaos based cancellable biometric template protection scheme using chaotic functions is proposed to address the above challenges. The chaotic functions give excellent pseudorandom sequences [64]. Conventional transformation algorithm like AES [69] involves large number of operations which will consume more time for transformation. Chaotic functions are deterministic and sensitive to the initial values. According to this feature, it has complex active action, which can be used to protect data content. For example, the random sequence produced by chaotic phenomenon can be used to encrypt data in secret communication. This property makes the initial value suitable for the key that controls the data encryption or decryption.

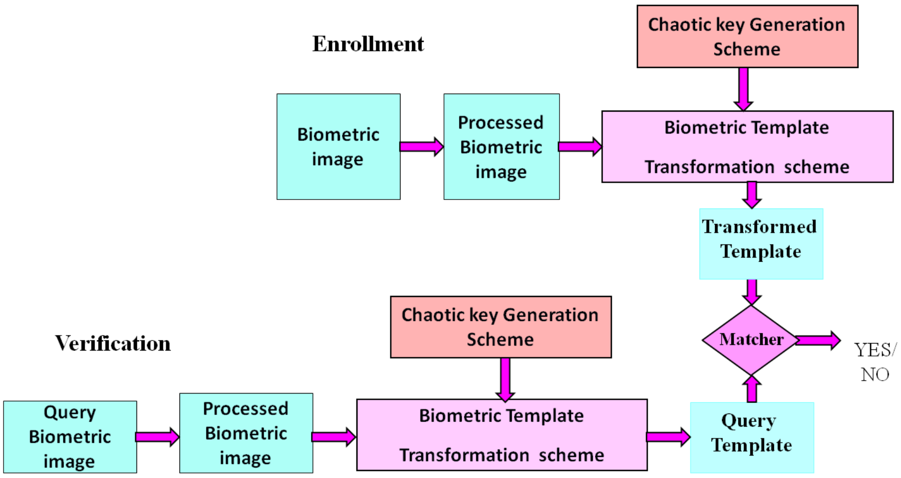
Enrollment
Chaotic key Generation Scheme
Biometric image
Processed Biometric image
Biometric Template Transformation scheme
Transformed Template
Verification
Chaotic key Generation Scheme
Matcher
YES/ NO
Query Biometric image
Processed Biometric image
Biometric Template Transformation scheme
Query Template

Figure 1: Over view of proposed template protection scheme

The model described in Fig. 1 captures user biometric characteristics by capturing device and processes as template during enrollment. The sample is then transformed using chaotic key streams derived from chaotic function and suitable cryptographic algorithm into a transformed biometric template. The transformed biometric template will provide a normalized, efficient and highly discriminating representation of the feature, which can then be compared with query template.

During verification, query biometric image is captured, processed as template and then transformed using same chaotic key streams derived during enrollment process and cryptographic algorithm. The transformed query template is matched with transformed template stored during enrollment in order to determine identity..

VI. SUITABILITY OF CCBT SYSTEM AS BIOMETRIC TEMPLATE PROTECTION SCHEME TO ADDRESS THE CHALLENGES

Chaotic functions are known to posses desirable properties to address the issues and challenges of CB and BC systems discussed in section 4. A chaotic system is a non-linear deterministic system so sensitive to initial conditions that it appears random.

6.1 Deterministic, means that they have some determining mathematical equations controlling their behavior.

To explain this property, let us consider one of the chaotic map equations, the logistic map as a reference which is represented in equation 2.

$$x_{n+1} = r * x_n [1 + x_n] \qquad (2)$$

Where x0 (n=0) is the initial value, r is the bifurcation parameter and depending on the value of r, x0 the dynamics of the generated chaotic sequence can change dramatically. The [1-xn] term serves to inhibit growth because as x approaches 1, [1-x_n] approaches 0. Plot of x_{n+1} verses x_n with r = 3 is as shown in figure 2, we can see that we have a non linear relation.

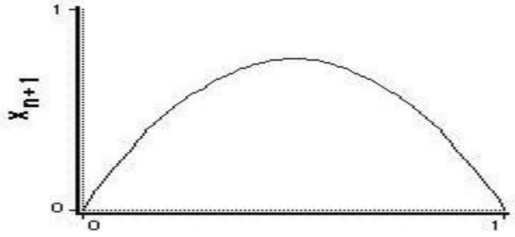

Figure 2: Limited growth (Verhulst) model. Xn+1 vs. X_n, r = 3

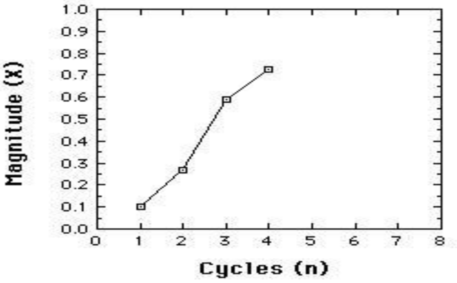

Figure 3: Behavior of the Logistic map for r = 3, x_1 = 0.1, iterated to give x_2, x_3, and x_4

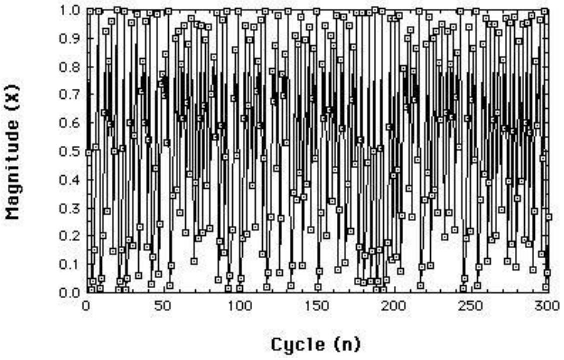

Figure 4: Chaotic behavior of the Logistic map at r = 3.99

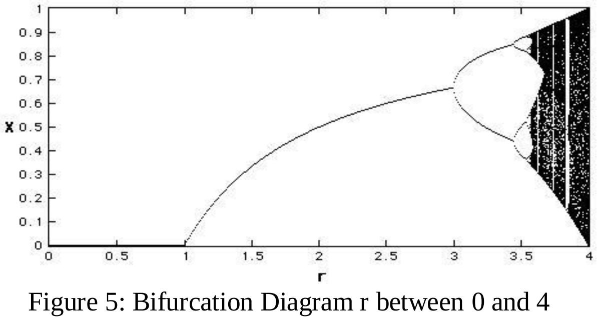

Figure 5: Bifurcation Diagram r between 0 and 4

The complete beaviour of the model can be seen by iterating equation 2. Suppose r = 3, and x1 = 0.1, then we get,

$x_2 = r * x_1[1-x_1] = 3 * (.1) * (.9) = 0.27$
$x_3 = r * x_2[1-x_2] = 3 * (.27) * (.73) = 0.591$
$x_4 = r * x_3[1-x_3] = 3 * (.591) * (.409) = 0.725$

From the plot in Fig.3 and Fig.4, it turns out that the logistic map is a very different function, depending on its control parameter r. To analyze this, it is examined for the time series produced at different values of r, starting near 0 and ending at r=4. Along the way it can be seen very different results, revealing and introducing major features of a chaotic system.

The Fig.5 shows the bifurcation diagram of the logistic map, r along the x-axis. A bifurcation diagram is a visual summary of the succession of period-doubling produced as r increases. For each value of r the system is first allowed to settle down and then the successive values of x are plotted for a few hundred iterations. It can be observed from bifurcation diagram that for r less than one, all the points are plotted at zero. Zero is the one point attractor for r less than one. For r between 1 and 3, we still have one-point attractors, but the 'attracted' value of x increases as r increases, at least to r = 3. Bifurcations occur at r=3, r=3.45, 3.54, 3.564, 3.569 (approximately), etc., until just beyond 3.57, where the system is chaotic. It can be observed, between 3.57 and 4 there is a rich interleaving of chaos and order. From this theoretical analysis it shows that, a small change in r can make a stable system chaotic, and vice versa.

In the proposed scheme, the bifurcation property of chaotic function for bifurcation factor r between 3 and 3.5 can be used to generate random, unpredictable key streams for biometric template transformation which addresses the challenge of preventing guessing of biometric keys.

6.2 Unpredictable and non-linear, means they are highly sensitive to initial conditions. Even a very slight change in the initial value can lead to entirely different outcomes.

Another important feature emerges in the chaotic region. To observe it, we compared the time series for x1=0.3 (in black) with that for x1=.3000001 (in blue) in figure 6 and Fig.7 provides scatter plots for the two series before and after 24 iterations which shows that correlation after 24 iterations (right side), is essentially zero.

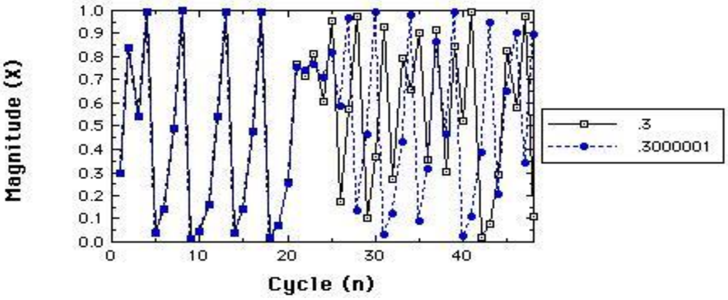

Figure 6: Two time series for r=3.99, x_1=.3 compared to x_1=.3000001

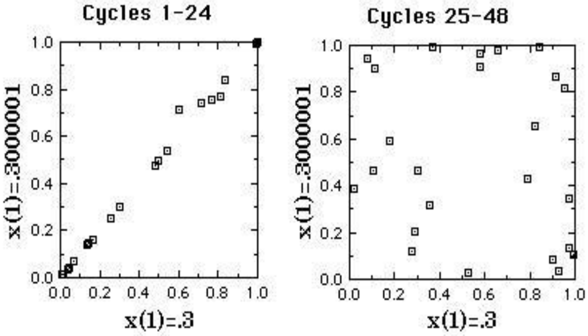

Figure 7: Scatter plots of series starting at 0.3 vs. series starting at 0.3000001.
The first 24 cycles on the left, next 24 on the right.

Fig. 6 and Fig.7 illustrates that, a chaotic system, even one determined by a simple rule, is in principle unpredictable. It is unpredictable, "in principle" because in order to predict its behavior into the future we must know its current value precisely. It is explained here with an example where a slight difference, in the sixth decimal place of initial value, resulted in prediction failure after 24 iterations. And six decimal places far exceeds the kind of measuring accuracy we typically achieve with natural biological systems.

This very high sensitivity to initial condition property of chaotic maps can be used in the proposed scheme to generate different transformed templates from same biometric data by very slight change in initial condition to generate key stream, so that different applications with different transformed templates appear random to themselves which addresses the challenge of unlinkability.

6.2 Very large key space and high entropy addresses the revocability of transformed templates.

In the proposed method, considering most commonly used 16 bit PC platform as an example and key streams = { k1, k2, k3} three different keys, with each key consisting of key = (x_0, r_0) (x_0= initial value and r_0= bifurcation factor), the expected key space size is $(10^{16})^6 \approx 2^{319}$, which is larger than the acknowledged most secured AES algorithm. With this key space, it is possible to generate very large number of keys which addresses the challenge of revocability. Also in the proposed scheme the expected entropy of transformed biometric template stored using chaotic maps is about 0.9991[76,77,72], which is close to the theoretical value(=1). This property provides privacy and security by providing it impossible to guess the keys..

VII. CONCLUSION

In this paper, chaotic maps are proposed to generate renewable and privacy preserving transformed biometric templates. The theoretical analysis shows that, very high key sensitivity and large key space properties of chaotic maps can be used to efficiently address the challenges in BCS and CB Systems. The proposed scheme can provide high-confidence cancelable biometric verification performance with very large renewability and Irreversibility properties.

REFERENCES

[1] Rathgeb and Uhi, A survey on biometric cryposystems and cancellable biometrics, EURASIP Journal on Information Security, 2011.

[2] Jain AK, Ross A, Prabhakar S: An introduction to biometric recognition.IEEE Trans Circ Syst Video Technol 2004, 14:4-20.

[3] AK Jain, K Nandakumar, A Nagar, Biometric template security. EURASIP J Adv Signal Process, 1–17 (2008)

[4] Y Luo, SS Cheung, S Ye, Anonymous biometric access control based on homomorphic encryption. ICME'09: Proc of the 2009 IEEE Int Conf on Multimedia and Expo, 1046–1049 (2009).

[5] U Uludag, S Pankanti, S Prabhakar, AK Jain, Biometric cryptosystems: issues and challenges. Proc IEEE 92(6), 948–960 (2004)

[6] A Cavoukian, A Stoianov, Biometric encryption. Encyclopedia of Biometrics (Springer, 2009)

[7] A Cavoukian, A Stoianov, Biometric encryption: the new breed of untraceable biometrics. Biometrics: Fundamentals, Theory, and Systems (Wiley, London, 2009)

[8] A K Jain, A Ross, U Uludag, Biometric template security: Challenges and solutions. Proc of European Signal Processing Conf (EUSIPCO) (2005)

[9] N K Ratha, JH Connell, RM Bolle, Enhancing security and privacy in biometrics-based authentication systems. IBM Syst J 40, 614–634 (2001)

[10] E A Verbitskiy, P Tuyls, C Obi, B Schoenmakers, B Ŝkorić, Key extraction from general nondiscrete signals. IEEE Trans Inf Forensic Secur 5(2), 269–279 (2010)

[11] A Juels, M Wattenberg, A fuzzy commitment scheme. 6th ACM Conf on Computer and Communications Security, 28–36 (1999)

[12] A Nagar, K Nandakumar, A Jain, A hybrid biometric cryptosystem for securing fingerprint minutiae templates. Pattern Recogn Lett 31, 733–741 (2010).

[13] C Rathgeb, A Uhl, Systematic construction of iris-based fuzzy commitment schemes. Proc of the 3rd Int Conf on Biometrics 2009 (ICB'09), 947–956 (2009) LNCS: 5558

[14] C Rathgeb, A Uhl, Context-based texture analysis for secure revocable iris-biometric key generation. Proc of the 3rd Int Conf on Imaging for Crime Detection and Prevention, ICDP '09 (2009)

[15] L Zhang, Z Sun, T Tan, S Hu, Robust biometric key extraction based on iris cryptosystem. Proc of the 3rd Int Conf on Biometrics 2009 (ICB'09), 1060–1070 (2009) LNCS: 5558

[16] T Ignatenko, F Willems, Achieving secure fuzzy commitment scheme for optical pufs. Int Conf on Intelligent Information Hiding and Multimedia Signal Processing, 1185–1188 (2009)

[17] C Rathgeb, A Uhl, Adaptive fuzzy commitment scheme based on iris-code error analysis. Proc of the 2nd European Workshop on Visual Information Processing (EUVIP'10), 41–44 (2010)

[18] A Goh, DCL Ngo, Computation of cryptographic keys from face biometrics. Communications and Multimedia Security, 1–13 (2003) (LNCS: 2828)

[19] M Ao, SZ Li, Near infrared face based biometric key binding. Proc of the 3rd Int Conf on Biometrics 2009 (ICB'09), 376–385 (2009) LNCS: 5558

[20] K Nandakumar, A fingerprint cryptosystem based on minutiae phase spectrum. Proc of IEEE Workshop on Information Forensics and Security (WIFS) (2010)

[21] H Lu, K Martin, F Bui, K Plataniotis, D Hatzinakos, Face recognition with biometric encryption for privacy-enhancing self exclusion. Proc of the 16th Int Conf on Digital Signal Processing (DSP 2009) (2009)

[22] E Maiorana, P Campisi, A Neri, User adaptive fuzzy commitment for signature templates protection and renewability. SPIE J Elec Imaging Spec Sect Biomet Adv Secur Usability Interoper 17(1), 1–12 (2008)

[23] IR Buhan, JM Doumen, PH Hartel, RNJ Veldhuis, Constructing practical fuzzy extractors using QIM, Centre for Telematics and Information Technology, University of Twente, Enschede, Technical Report TR-CTIT-07-52

[24] TC Clancy, N Kiyavash, DJ Lin, Secure smartcard-based fingerprint authentication. Proc ACM SIGMM 2003 Multimedia, Biometrics Methods and Applications Workshop, 45–52 (2003)

[25] K Nandakumar, AK Jain, S Pankanti, Fingerprint-based fuzzy vault: implementation and performance. IEEE Trans Inf Forensic Secur 2, 744–757 (2007)

[26] D Moon, W-Y Choi, K Moon, Y Chung, Fuzzy fingerprint vault using multiple polynomials. IEEE 13th Int Symposium on Consumer Electronics, ISCE '09, 290–293 (2009)

[27] A Nagar, S Chaudhury, Biometrics based Asymmetric Cryptosystem Design Using Modified Fuzzy Vault Scheme. 18th Int Conf on Pattern Recognition (ICPR'06) ICPR 4, 537–540 (2006)

[28] A Nagar, K Nandakumar, AK Jain, Securing fingerprint template: Fuzzy vault with minutiae descriptors. Int Conf on Pattern Recognition (ICPR'08). IEEE, 1–4 (2008)

[29] A Arakala, Secure and private fingerprint-based authentication. Bull Aust Math Soc 80, 347–349 (2009).

[30] A Kumar, A Kumar, A palmprint based cryptosystem using double encryption. Proc SPIE Conf Biometric Technology for human identification 6944, 69440D-1–69440D-9 (2008)

[31] A Kumar, A Kumar, Development of a new cryptographic construct using palmprint-based fuzzy vault. EURASIP J Adv Signal Process, 11 (2009)

[32] A Goh, ABJ Teoh, DCL Ngo, Random multispace quantization as an analytic mechanism for biohashing of biometric and random identity inputs. IEEE Trans Pattern Anal Mach Intell 28(12), 1892–1901 (2006).

[34] A Kong, K-H Cheunga, D Zhanga, M Kamelb, J Youa, An analysis of BioHashing and its variants. Pattern Recogn 39, 1359–1368 (2006).

[35] ABJ Teoh, YW Kuan, S Lee, Cancellable biometrics and annotations on biohash. Pattern Recogn 41(6), 2034–2044 (2008).

[36] A Lumini, L Nanni, An improved biohashing for human authentication. Pattern Recogn 40(3), 1057–1065 (2007).

[37] L Nanni, A Lumini, Random subspace for an improved biohashing for face authentication. Pattern Recogn Lett 29(3), 295–300 (2008).

[38] K Nandakumar, AK Jain, Multibiometric template security using fuzzy vault. IEEE 2nd Int Conf on Biometrics: Theory, Applications, and Systems, BTAS '08, 1–6 (2008)

[39] K Voderhobli, C Pattinson, H Donelan, A schema for cryptographic key generation using hybrid biometrics. 7th annual postgraduate symp.: The convergence of telecommunications, networking and broadcasting, Liverpool (2006)

[40] S Kanade, D Petrovska-Delacretaz, B Dorizzi, Multi-biometrics based cryptographic key regeneration scheme. IEEE 3rd Int Conf on Biometrics: Theory, Applications, and Systems, BTAS '09, 1–7 (2009)

[41] S Kanade, D Camara, D Petrovska-Delacrtaz, B Dorizzi, Application of biometrics to obtain high entropy cryptographic keys. Proceedings of World Academy on Science, Engineering, and Technology, Hong Kong 52 (2009)

[42] VS Meenakshi, G Padmavathi, Security analysis of password hardened multimodal biometric fuzzy vault. Proceedings of World Academy of Science, Engineering and Technology 56 (2009)

[43] A Jagadeesan, T Thillaikkarasi, K Duraiswamy, Cryptographic key generation from multiple biometric modalities: Fusing minutiae with iris feature. Int J Comput Appl 2(6), 16–26 (2010)

[44] M Zhang, B Yang, W Zhang, T Takagi, Multibiometric based secure encryption and authentication scheme with fuzzy extractor. Int J Netw Secur 12(1), 50–57 (2011)

[45] F Chafia, C Salim, B Farid, A biometric crypto-system for authentication. Proc of Int Conf on Machine and Web Intelligence (ICMWI), 434–438 (2010)

[46] H Chen, H Sun, K-Y Lam, Key management using biometrics. Int Symposium on Data, Privacy, and E-Commerce 1, 321–326 (2007)

[47] FM Bui, K Martin, H Lu, KN Plataniotis, D Hatzinakos, Fuzzy key binding strategies based on quantization index modulation (QIM) for biometric encryption (BE) applications. Trans Inf Forensic Secur 5, 118–132 (2010)

[48] IR Buhan, JM Doumen, PH Hartel, RNJ Veldhuis, Fuzzy extractors for continuous distributions. University of Twente, Technical Report (2006)

[49] EJC Kelkboom, J Breebaart, I Buhan, RNJ Veldhuis, Analytical template protection performance and maximum key size given a Gaussian modeled biometric source. Proc of SPIE defense, security and

[50] T Ignatenko, FMJ Willems, Information leakage in fuzzy commitment schemes. Trans Inf Forensic Secur 5(2), 337–348 (2010)

[51] J Zuo, NK Ratha, JH Connel, Cancelable iris biometric. Proc of the 19th Int Conf on Pattern Recognition 2008 (ICPR'08), 1–4 (2008)

[52] M Savvides, B Kumar, P Khosla, Cancelable biometric filters for face recognition. ICPR '04: Proc of the Pattern Recognition, 17th Int Conf on (ICPR'04) 3, 922–925 (2004).

[53] J Hämmerle-Uhlr, E Pschernig, A Uhl, Cancelable iris biometrics using block re-mapping and image warping. Poc of the Information Security Conf 2009 (ISC'09) LNCS 5735, 135–142 (2009)

[54] NK Ratha, JH Connell, S Chikkerur, Generating cancelable fingerprint templates. IEEE Trans Pattern Anal Mach Intell 29(4), 561–572 (2007).

[55] P Färberböck, J Hämmerle-Uhl, D Kaaser, E Pschernig, A Uhl, Transforming rectangular and polar iris images to enable cancelable biometrics. Proc of the Int Conf on Image Analysis and Recognition (ICIAR'10) (Springer LNCS, 2010) 6112, pp. 276–386

[56] C Rathgeb, A Uhl, Secure iris recognition based on local intensity variations. Proc of the Int Conf on Image Analysis and Recognition (ICIAR'10) (Springer LNCS, 2010) 6112, pp. 266–275

[57] E Maiorana, P Campisi, J Fierrez, J Ortega-Garcia, A Neri, Cancelable templates for sequence-based biometrics with application to on-line signature recognition. Trans Syst Man Cybernet A Syst Hum 40(3), 525–538 (2010)

[58] T Boult, Robust distance measures for face-recognition supporting revocable biometric tokens. FGR '06: Proc of the 7th Int Conf on Automatic Face and Gesture Recognition, 560–566 (2006).

[59] T Boult, W Scheirer, Bio-cryptographic protocols with bipartite biotokens. Proc of the IEEE Biometric Symposium, BSYM '08, 9–16 (2008)

[60] O Ouda, N Tsumura, T Nakaguchi, Bioencoding: a reliable tokenless cancelable biometrics scheme for protecting iris codes. IEICE Trans Inf Syst E93.D, 1878–1888 (2010).

[61] O Ouda, N Tsumura, T Nakaguchi, Tokenless cancelable biometrics scheme for protecting iris codes. Proc of the 20th Int. Conf. on Pattern Recognition (ICPR'10), 882–885 (2010)

[62] JK Pillai, VM Patel, R Chellappa, NK Ratha, Sectored random projections for cancelable iris biometrics. Proc of the IEEE Int Conf. on Acoustics Speech and Signal Processing (ICASSP), 1838–1841 (2010)

[63] B Yang, C Busch, D Gafurov, P Bours, Renewable minutiae templates with tunable size and security. Proc of the 20th Int Conf on Pattern Recognition (ICPR'10), 878–881 (2010)

[64] B Yang, D Hartung, K Simoens, C Busch, Dynamic random projection for biometric template protection. Proc of the 4th IEEE Int Conf on Biometrics: Theory, applications and systems (BTAS'10), 1–7 (2010)

[65] S Hirata, K Takahashi, Cancellable biometrics with perfect secrecy for correlation-based matching. Proc of the 3rd Int Conf on Biometrics 2009 (ICB'09), LNCS 5558, 868–878 (2009)

[66] K Takahashi, S Hirata, Generating provably secure cancelable fingerprint templates based on correlation-invariant random filtering. IEEE 3rd Int Conf on Biometrics: Theory, Applications, and Systems, BTAS '09, 1–6 (2009)

[67] J Bringer, H Chabanne, B Kindarji, Anonymous identification with cancelable biometrics. Proc of the 6th Int Symposium on Image and Signal Processing and Analysis, ISPA '09, 494–499 (2009)

[68] EJC Kelkboom, GG Molina, J Breebaart, RNJ Veldhuis, TAM Kevenaar, W Jonker, Binary biometrics: an analytic 22 framework to estimate the performance curves under Gaussian assumption. Trans Syst Man

[69] A. Juels and M. Sudan. A Fuzzy Vault Scheme. In IEEE International Symposium Information Theory, pp- 408-413, 2002.

[70] Jiancheng Zou, ChangZhen Xiong, Dongxu Qi, Rabab K. Ward," The Application of Chaotic Maps in Image Transformation", Proc. IEEE 2005.

[71] C Chong Fu,Zhiliang Zhu, "A Chaotic Image transformation scheme based on circular bit space shift method", The 9th International Conference for Young Computer Scientists, IEEE Computer Society, pp. 3057 – 3061, 2008

[72] Supriya V G, Malini M Patil, Dileep Dharmappa, "Chaos Based Biometric Template Protection Scheme", 2010 3rd International Conference on Machine Vision, December 2010,IEEE Catalog Number CFP1032D-PRT, ISBN: 978-1-4244-8888-9.

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

[74] T. Monoth and A. P. Babu, Recursive Visual Cryptography Using Random Basis Column Pixel Expansion,. in Proceedings of IEEEInternational Conference on Information Technology, 2007, pp. 41-43.

[75] Reena Mary George, Facial Template Protection Using Extended Visual Cryptography and Chaotic Encryption, International journal of technology enhancements and emerging engineering research, vol 1, issue 4, ISSN 2347-4289, Copyright © 2013 IJTEEE.

[76] Ameer A. Mohammed Baqer, and Suhas H. Patil 2, Efficient Iris Biometrics Technique for Secure Distributed Systems, IJCSNS International Journal of Computer Science and Network Security, VOL.13 No.2, February 2013

[77] Prof. Maithili Arjunwadkar, Prof. Dr. R. V. Kulkarni, International Journal of Computer Applications (0975 – 8887) Volume 3 – No.6, June 2010