Multimed Tools Appl
DOI 10.1007/s11042-015-2933-6

Biometric template protection using cancelable biometrics and visual cryptography techniques

Harkeerat Kaur[1] · Pritee Khanna[1]

Received: 15 January 2015 / Accepted: 1 September 2015

Abstract Wide spread use of biometric based authentication implies the need to secure biometric reference data. Various template protection schemes have been introduced to prevent biometric forgery and identity thefts. Cancelable biometrics and visual cryptography are two recent technologies introduced to address the concerns regarding privacy of biometric data, and to improve public confidence and acceptance of biometric systems. Cancelable biometrics is an important technique that allows generation of revocable biometric templates. As the number of biometric instances are limited and once compromised they are lost forever. Cancelable biometrics allows templates to be cancelled and revoked like passwords innumerable times. Recently, various approaches that utilize visual cryptography to secure the stored template and impart privacy to the central databases have been introduced. This work attempts to summarize the existing approaches in literature making use of these two technologies to protect biometric templates.

Keywords Biometric template protection · Cancelable biometrics · Biometric salting · Non-invertible transforms · Visual cryptography · Visual secret sharing

1 Introduction

Biometric identification technology is based on recognizing an individual from his/her distinct physical or behavioral characteristics like face, fingerprint, iris, voice, retina scan, etc. It is an automated process of identification and authentication, in which specific biometric

✉ Pritee Khanna
pkhanna@iiitdmj.ac.in

Harkeerat Kaur
harkeerat.kaur@iiitdmj.ac.in

[1] PDPM Indian Institute of Information Technology, Design and Manufacturing, Jabalpur 482005, Madhaya Pradesh, India

Published online: 19 October 2015

traits of an individual are extracted during enrollment and stored in the form of biometric templates. Later, verification and authentication is performed by matching the input template provided by the user and the stored templates [34]. The goal is to provide access at physical and logical levels. Biometric based identification has proven to be a robust and accurate tool in recent times, replacing the conventional password/PIN based identification systems. Biometric based human recognition has opened ways to many new possibilities, but at the same time it is not perfectly secured and unsusceptible to attacks. Several types of abuses of biometrics are described by Schneier [83]. Unsupervised biometric applications and web based applications provide attackers ample time and opportunities to intercept the system and gain unauthorized access. Details about security issues, vulnerable points and attacks are provided in [5, 35, 73, 77].

Such situations are leading to a growing gap between the increasing yet conflicting demands of "security and privacy using biometric applications" and "biometric data protection". To bridge this gap, biometric template protection schemes are required to protect the biometric data/feature and at the same time, maintain capability to identify and verify identity. This paper examines approaches to generate protected biometric templates using two recent technologies, cancelable biometrics and visual cryptography.

The paper is organized as follows: Section 2 briefly discusses the requirement, methodology, and challenges encountered while providing biometric template protection. Section 3 discusses template protection using cancelable biometrics. Section 4 provides details of visual cryptography approaches for securing biometric template. Attempts are made to comprehensively cover various issues concerning requirements, performance, vulnerabilities, and attacks for both the technologies.

2 Biometric template protection

Biometric data is a success for granting access control in various commercial applications such as ATMs, credit cards, bank accounts, government applications such as ID cards, passports, visa, electronic voting, and a number of forensic applications. While the use of biometric templates is easy, convenient, and reliable, there are some security and privacy related issues that need to be addressed:

1. *Impersonation/Identity theft:* If the biometric data of a person is lost it can be used by an adversary to gain illegitimate access to his accounts/services. For example, an attacker can covertly uplift the latent fingerprints of a user from an object and reconstruct its physical/digital artifact.
2. *Sensitivity:* Besides uniquely identifying an individual, biometric data reveals a lot of personal and sensitive information about the person such physical illness and medical conditions.
3. *Linkability:* Biometric data are being increasingly shared leading to tracing and tracking of users across different databases by matching their reference templates. This cross matching of databases to determine relation between stored reference templates needs to be prevented.
4. *Loss of biometrics is permanent:* The number of biometrics is limited and their compromise/theft can render it useless for the entire lifetime of a user.

These issues increase the need for protecting the template by not storing them in the format in which they are obtained from a user. Biometric template protection suggests use of some auxiliary/helper data to transform the reference biometric data into a new format such that the above mentioned concerns can be addressed. At the same time, these transformed templates must not compromise the ability to identify/verify individuals, maintain discriminability and intra-user variability, and address various attack scenarios. Some standards established for evaluating the biometric template protection are ISO/IEC 24745: Biometric information protection, ITU-T X.1088: Telebiometric digital key framework, and ITU-T X.1090: Authentication framework with one-time telebiometric template. To protect the biometric information, ISO/IEC 24745 : 2011 provides guidelines for various requirements under confidentiality, integrity, and renewability/revocability during storage and transfer [100]. Figure 1 depicts ISO/IEC 24745 : 2011 architecture for biometric template protection, where M is the observed biometric data during enrollment, M' is the probe biometric data, and V is the comparison result. A Protected Template (PT) consists of a Pseudonymous Identifier (PI) and possibly a helper or Auxiliary Data (AD). The PI represents the individual in an application context and is used as a reference for verification, but does not allow retrieval of the enrolled data. AD is a public data that does not reveal any significant information about the biometric template but is needed at the time of verification to reconstruct the original PI. The features extracted during enrollment are fed into a Pseudonymous Identifier Encoder (PIE) system which produces a renewable biometric reference consisting of a PI and AD. During verification, Pseudonymous Identifier Recoder (PIR) recodes a new pseudonymous identifier PI' from a freshly captured sample and AD. The Pseudonymous Identifier Comparator (PIC) compares the recoded PI' with the reference PI to generate a match. There are different levels at which a biometric template can be secured, e.g., hardware level, software level, and protocol level. Figure 2 depicts the classification, and approaches that exist at various levels, and Table 1 summarize key template protection schemes existing in literature. These schemes have offered promising solutions to protect biometric template at various levels and types of attack.

Fuzzy commitment [37], fuzzy vaults [60], and secure sketches [50, 94] are some techniques in biometric cryptosystems [90, 104] to secure the biometric template stored in a database or to protect the transfer of templates over web based applications. Biometric encryption is one of the major categories for template protection which monolithically combines a cryptographic key with the template. However, security of biometric encryption techniques depends entirely on the secrecy of the encryption or secret key. Hence, the

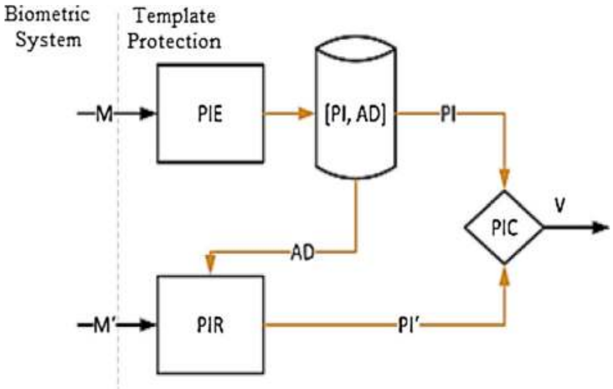


Fig. 1 ISO/IEC architecture for biometric template protection [100]

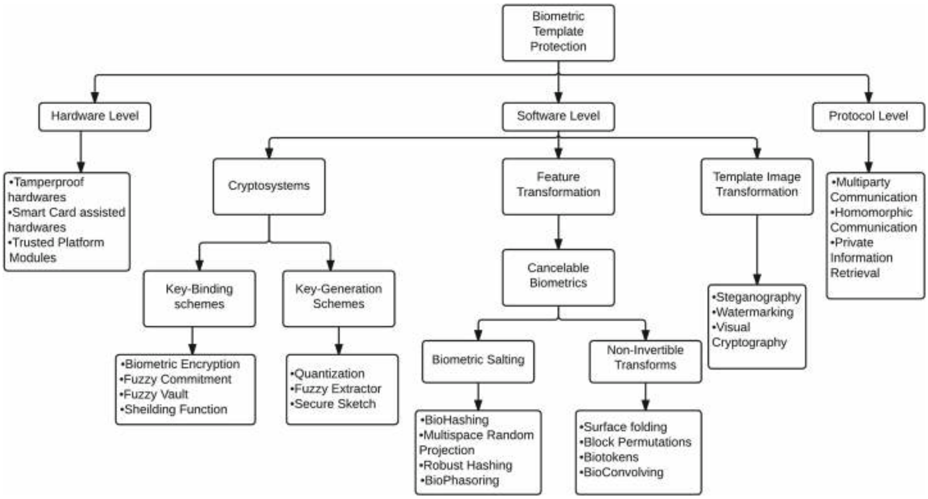


Fig. 2 A classification of various biometric protection techniques

system is as good as the password based system in which entire data is available if the key is shared or stolen. Cancelable biometrics enhances template protection by ensuring unlinkability and revocability/renewability. Cancelable biometrics provides template level protection by generating transformed templates which can be cancelled like passwords. Protection schemes like watermarking, steganography, and visual cryptography techniques protect templates at image level. Watermarking finds applications in asserting ownership, detecting tampers, and data integrity. Steganography communicates secret information by hiding it in multimedia carrier like image/video/audio files. Visual cryptography is a branch of cryptography that divides image into meaningless shares and distributes between users. It can be used to provide privacy to the biometric image templates stored in central databases.

3 Cancelable biometrics

Passwords can be renewed innumerable times, whereas a biometric data once compromised, becomes obsolete for the entire lifetime of a user. To alleviate this problem, Soutar et al. [90] took initiatives to generate renewable and revocable biometric templates, but Ratha et al. [73] explored the idea. Cancelable biometrics allows biometric templates to be revoked and renewed like a password and at the same time being unique to every application. It is one of the major template protection schemes besides biometric cryptosystems. Cancelable biometrics is defined as “a set of intentional, systematical and repeated distortions on the biometric feature in order to protect the user specific sensitive information by not storing and matching them in the original format”.

Renewability is defined as “The property of a transform or a process to generate multiple, independent, and transformed biometric samples obtained from the same data subject and which can be used to recognize the individual while not revealing information about the original reference (ISO 24745)”. If a cancelable feature is compromised, the distortion

Table 1 Key biometric template protection schemes

Technique	**Author(s)**	**Modality**	**FRR/FAR(%)**	**Pseudonymous Identifier**	**Auxiliary Data**
BioConvolving	Maiorana et al. [52]	Signature	10.81 ERR	Transformed template	Decomposition key
BioHashing	Connie et al. [15]	Palmprint	0.0/0.0	A robust binary string	Random projection matrix
	Teoh et al. [100]	Face	0.0/0.0		
BioScrypt	Soutar et al. [91]	Fingerprint	-	Cryptographic key	Filter and key link
Block Permutation	Ratha et al. [74]	Fingerprint	$35/10^{-4}$	Transformed template	Transformation parameters
Surface Folding	Ratha et al. [74]	Fingerprint	$15/10^{-4}$	Transformed template	Transformation parameters
Fuzzy Commitment	Hao et al. [29]	Iris	0.42/0.0	Hash of secret string	Offset
	Bringer et al. [8]	Iris	5.62/0.0	Hash of secret string	Offset
Fuzzy Vault	Clancy et al. [14]	Fingerprint	20-30/0.0	Hash of secret string	Point set
	Nandakumar et al. [60]	Fingerprint	4.0/0.004	Hash of secret string	Point set
	Wu et al. [108]	Iris	5.5/0.0	Hash of secret string	Point set
Quantization	Feng & Wah [21]	Signature	28.0/1.2	Hash of secret string	Quantization errors
	Vielhauer et al. [105]	Signature	7.05/0.0	Hash of secret string	Quantization errors

characteristics are changed, and the same biometrics is mapped to a new template (renewed) which can be used subsequently. The objectives of cancelable biometric scheme are [82]:

1. *Diversity:* Many cancellable templates can be generated from the same biometric for different applications.
2. *Renewability/Revocability:* Straightforward revocation and reissue in case the template is compromised.
3. *Non-invertibility:* To prevent forgery it should not be possible to obtain information about the original biometric feature from the transformed template.
4. *Performance:* The recognition performed with transformed template should not deteriorate the performance of the system. It should also possess backward compatibility.

Cancelable biometrics requires storage of the distorted version of the biometric template. It provides high level privacy by allowing multiple templates to be associated with the same biometric data. At every enrollment a different transformation can be followed to generate the protected template. This helps to promote non-linkability of user's biometric data stored across various databases. Transformations can be applied at two levels to generate cancelable templates- *Signal level* and *Feature level*. The transformations applied are such that the inversion of the transformed template to recover the original template is infeasible by any potential attacker, thereby promoting irreversibility. Also, the transformed templates must preserve the distinguishing properties of the feature vectors at signal or feature levels, thereby maintaining the functional performance of the system.

3.1 Cancelability requirements of a transform

Successful transformation of a biometric template into a cancelable one requires an appropriate transformation function. The implementation of a transformation needs to meet the following requirements for ensuring performance [74]:

1. *Registration:* Cancelable transform to be repeatable on more than one instance of the same biometric requires the features to be measured with respect to the same coordinate system. On registration the distinguishing points (features) of transformed templates should overlap as well as possible.
2. *Intra-user variation tolerance:* The intra-user variation is another important aspect that needs to be focused. Biometric templates of a person that match in original domain must also match after transformation. The transformed features must be robust with respect to variations and must not critically increase False Reject Rate (FRR).
3. *Entropy retention:* The intrinsic strength (individuality) of the biometric template should not be lost after the transformation. It should be comparable to the original biometric template. This constraint prevents False Acceptance Rate (FAR) to increase while the system operates in the transformed domain.
4. *Transformation function design:* The transformation function is required to satisfy the following conditions:
   (a) The original biometric template should not match with the transformed one.
   (b) Different transforms of the same user should not match with each other.
   (c) To ensure the privacy of the transformed template it should not be possible to recover the original biometric by inverse transformation.

3.2 Template transformation techniques

As stated earlier, cancelable biometrics involves distortion of biometric data at signal or feature level. At the signal level, the distortions are performed directly on the data collected at the sensors, whereas at the feature level the extracted feature set is made to undergo certain distortions. Many simple techniques, like grid morphing and block permutations are applied to distort the original biometric at the signal level [73]. Biometric salting and non-invertible transforms are two main categories of template transformation. Techniques have been proposed for various modalities such as fingerprint, face, palmprint, iris, retina, finger vein, knuckle print, and electrocardiogram (ECG) features. A modality wise classification of the existing approaches along with the experimental results is provided in Table 2.

3.2.1 Biometric salting

Biometric salting works on the same principle of salting as in cryptography, but for transforming biometric templates. Salting blends an independent input factor such as user specific secret key (auxiliary data, e.g., random numbers or passwords) with the biometric data; and with the help of some transformations produces distorted templates. Auxiliary data is obtained externally, and it interacts directly with the biometric to increase the entropy of the template, thus making it difficult for an adversary to make a guess. In case of a compromise, it is easy to revoke and generate a new template by changing auxiliary data. However, since the transformations are invertible, accuracy and vulnerability of the scheme depends upon the confidentiality of auxiliary data.

BioHashing proposed by Teoh et al. [100] is an instance of biometric salting in which a Tokenized (pseudo) Random Number (TRN) is combined with biometric features to generate BioCodes. Figure 3 illustrates the BioHashing process. At the time of enrolment, auxiliary data is used to generate a user specific random matrix. The columns of this matrix are orthonormalized using Gram-Schmidt orthonormalization process, and the original biometric feature is transformed by projecting it along the columns of the orthonormalized random matrix. The transformed template is then binarized to generate BioCode by comparing it with a fixed threshold value. Binarization, a many to one mapping, helps in achieving irreversibility. Instead of the original biometric, the generated BioCode is stored in the database, and the user specific random data is provided to the enrollee as a token [99, 101]. For positive authentication a genuine user needs to provide his/her original biometric data and the token. In case the stored BioCode is intercepted, a new one can be generated by changing the token. An individual can have many BioCodes for different applications by having various tokens. BioHashing has been experimentally verified for fingerprint, face, palmprint, iris, and voice. It is reported to achieve nearly zero Equal Error Rates (ERR) for these modalities which is a substantial increase in performance. But, if an adversary gains an access to the transformed template and random data (token stolen), he can generate a coarse approximation of the original template as the process is invertible. Hence, the security of the data may be compromised and performance regresses.

Sutcu et al. [93] proposed robust hashing technique which uses non-invertible transforms involving nonlinear operations to improve the security of template. However there exists a tradeoff between discriminability and achieving non-invertibility using this technique.

Teoh et al. [97] proposed BioPhasoring to address the invertibility issue. The technique generates a set of complex vectors where the original vectors form the real part and rows

Table 2 Experimental results obtained with various cancelable biometric approaches

Modality	Author(s)	Technique	Database	FRR/FAR(%)
Fingerprint	Teoh et al. [100]	BioHashing	FVCDB1	0 ERR
	Ang et al. [1]	Key based geometric transform	FCV2002	4 ERR
	Tulyakov et al. [102]	Symmetric hashing	FVC2002	25.9/0
	Teoh et al. [97]	BioPhasor	FVC2004	5.31 ERR
	Ratha et al. [72]	Non-invertible transforms	Private database	$15/10^{-4}$
	Lee et al. [44]	Minutiae based bit strings	FVC2004	0 ERR
Face	Savvides et al. [82]	Random convolution	CMU-PIE	4.64/0
	Jeong et al. [36]	Random scrambling	AR	14 ERR
	Teoh [101]	BioHashing	ORL	0 ERR
	Kim et al. [39]	Extended random projections	AR Group I	18.469 ERR
Palmprint	Connie et al. [15]	BioHashing	Private database	0 ERR
	Leng et al. [47]	Randomized Gabor filter	PolyU	0.528 ERR
	Li et al. [49]	Chaotic stream cipher	PolyU	0.07 ERR
Iris	Zuo et al. [114]	Biometric salting	MMU1	$0.005/<10^{-3}$
	Hammerle-Uhl et al. [28]	Non-invertible transforms	CASIA V3	1.3 ERR
Voice	Xu et al. [111]	Non-invertible transforms	Private database	-
	Xu and Cheng [110]	Non linear transformation	CADCC	-
Retina	Pabitha and Latha[65]	Non-invertible constructions	DRIVE	0 ERR
Signature	Maiorana et al. [52]	BioConvolving	MYCT	10.81 ERR
Fingervein	Hirata and Takahashi [31]	Number theoretic transform	-	-
	Chen et al. [11]	Chaotic random projection	-	-
KnuklePrint	Belguechi et al. [3]	BioHashing	PolyU FKP	0 ERR
ECG	Dey et al. [17]	BioHashing	Private database	0 ERR

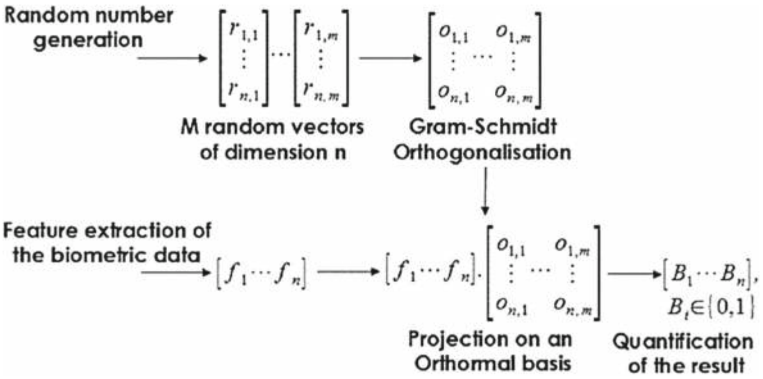

Random number generation
M random vectors of dimension n
Gram-Schmidt Orthogonalisation
Feature extraction of the biometric data
Projection on an Orthormal basis
Quantification of the result
$B_i \in \{0,1\}$

Fig. 3 BioHashing process [4]

of the orthonormal random vector form the imaginary part. This way BioPhasoring keeps on mixing user specified TRN with the biometric data iteratively and straight forward revocation is possible by token replacement. Secure hashing of dynamic hand signatures using biophasor mixing and discretization for cancelable keys generation is given in [40].

Teoh and Yaung [98] proposed Multispace Random Projection (MRP), a variant of BioHashing, to address the stolen token scenario. MRP extracts a fixed length feature vector from the raw biometric template and projects it on a non-invertible random subspace multiple times. Lumini and Nanni [51] suggested an improvement in BioHashing by utilizing a combination of MRP, different threshold values and fusion of scores. Multiple high dimension random projection [39], shifted random orthonormal transformation [107], one-time face template [45], augmented random projection [89], combination of BioHashing and BioPhasor [62], and random projections and sparse representations [66] are other variants of user specific random projections to generate robust cancelable templates.

Savvides et al. [82] proposed another instance of biometric salting for generating cancelable face templates using Minimum Average Correlation Energy (MACE) filter and random kernels. They demonstrated that convolving the training images with any random convolution kernel prior to building the biometric filter does not change the resulting correlation output peak-to-side lobe ratios, and thus preserves the authentication performance. However, the security may be jeopardized via a deterministic de-convolution with a known random kernel. To enhance security features of this method, correlation-based matching algorithm using number theoretic transform is proposed by Hirata and Takahashi [31]. It requires application of number theoretic transform on the biometric data before convolution with random kernels. Leng et al. [47] generated cancelable PalmCode from texture features obtained by randomized Gabor filters. In these techniques random kernels and random filters are generated with the help of user specific TRN.

Zuo et al. [114] proposed two new salting methods for generating cancelable iris templates- GRAY salting and BIN salting. GRAY salting (template based salty noise) consists of adding a unique random pattern (noise) or a synthetic iris texture to the Gabor features, and generating a new code according to a new texture. Similarly, BIN salting (code based salty noise) adds noisy patterns or random synthetic iris code on the original iris code to protect it. GRAY and BIN salting techniques are depicted in Fig. 4.

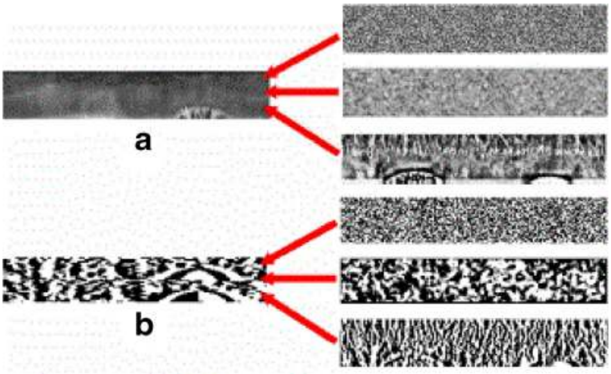
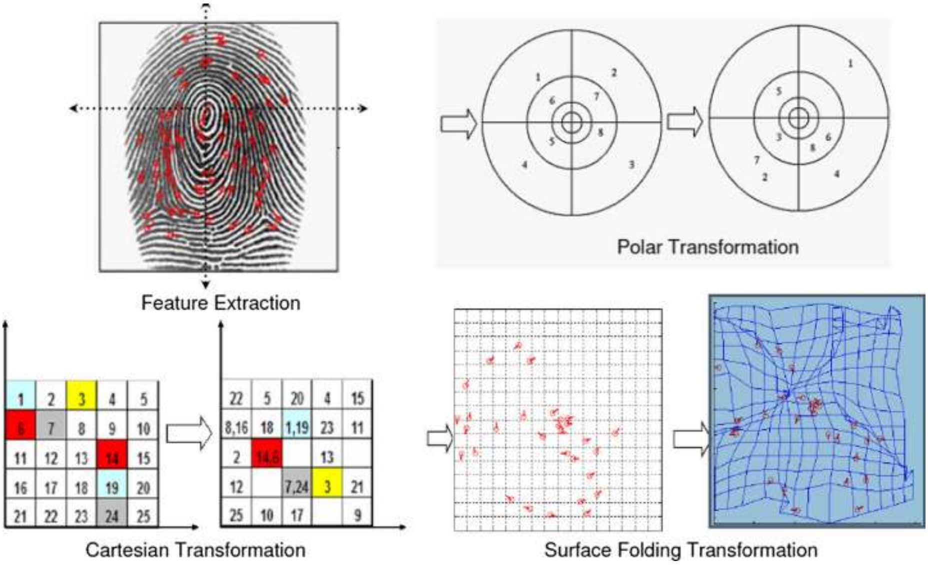


Fig. 4 Methodology of **a** GRAY salting **b** BIN salting [114]

3.2.2 Non-invertible transforms

Non-invertible transformation functions are one way surjective functions that are easy to compute but hard to inverse. These transforms are used to modify the biometric data into a new form within the context of signal or feature domain. A key/parameter is specifically required to be associated with the transformation function during enrollment, and the same key/parameter is used at every authentication of the instance. In case the template is compromised, a new one can be generated by simply changing the parameter or even the transformation function itself. The security of the techniques lies in the fact that even if the key and/or the transformed template are stolen, it is computationally hard for an adversary to obtain the original biometric data. To maintain a balance between discriminability and non-invertibility is a major challenge while designing these transformation functions. A realization of non-invertible transform reported by Ratha et al. in [72] is shown in Fig. 5. A fingerprint data can be transformed by a sequence of three non-invertible transformation functions (Cartesian, polar, and surface folding transformation) on the minutiae positions [72]. Cartesian transformation refers to tessellating the minutiae space into a rectangular grid. Within each cell of the grid, the minutiae points are measured with respect to the rectangular coordinate system. Distortion consists of a random many to one permutation of cells, where more than one cell can map to the same cell in the transformed domain. In polar (radial) transformation, the feature space is tessellated into sectors and minutiae points are measured in polar coordinate system rather than Cartesian coordinate system. The transformation requires a mapping key, which governs the radial transformation of the sectors so that they are not very different from each other. The surface folding transformations consists of Guassian kernels and electric potential field functions parametrized by random charge distribution for transforming the feature space. To achieve non-invertibility, all these transformation functions follow many to one mapping, which may lead to distortions to an extent that the discriminability of the system may be compromised, especially if the point crosses a certain boundary.

Tulyakov et al. [102] proposed symmetric hash functions (polynomials) for distorting minutiae information. The hash functions were irreversible because of their one way characteristics, and in the case of compromise new templates can be issued by changing the hash functions.



1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20
21	22	23	24	25

22	5	20	4	15
8,16	18	1,19	23	11
2	14,6		13	
12		7,24	3	21
25	10	17		9

Fig. 5 Non-invertible transformation technique by Ratha et al. [72]

Ang et al. [1] proposed key dependent algorithms based on geometric transformations to generate cancelable fingerprint templates. The technique requires locating the core point of the fingerprint image, and dividing it into two halves by a line. The angle of the line that divides the image depends on the key transformation function, so the new templates can be generated by simply changing the key values. The minutiae points reflected symmetrically about the line make it computationally hard to get the inverse transformation.

Boult et al. [7] proposed Biotokens, a cryptographically secure technique, divides the datum into two parts. One part is used for encoding purpose and the other for approximating a match and supporting robust distance computation. Farooq et al. [20] presented a concept of generating cancelable bit strings from fingerprint by extracting translational and rotational invariants minutiae triplets. On the same line, Lee et al. [44] proposed minutiae based bit strings to generate cancelable fingerprint templates. The technique requires mapping of minutiae into a predefined 3-D array consisting of small cells and determines which cell includes the minutiae points. The bit stings are generated by sequentially visiting the cells and assigning 1 to the cells containing more than one minutiae points, or 0 otherwise. 1-D bit strings are subjected to some random permutation determined by user specific PIN.

Zuo et al. [114] proposed new cancelable iris methods by operating on iris image or binary iris feature vector. Template based row shift and combinations (GRAY-COMBO) on unwrapped images is performed by selecting any two rows at random and combining them to form a new row by binary XOR or NXOR, where each row can be used more than once to ensure non-invertibility. Similar transform-code based row shift and combination (BIN-COMBO) can be applied to binary iris code to generate cancelable templates. Hämmerle-Uhl et al. [28] utilized block remapping and image warping procedures to generate cancelable iris templates.

Xu et al. [110, 111] proposed cancelable voice templates, where a non-invertible transformed version of the original voiceprint is generated by chaff point mixture method.

Maiorana et al. [53, 54] proposed BioConvolving, a convolution based non-invertible transformation technique. BioConvolving requires a biometric template to be expressed as a set of discrete finite sequences related to the temporal, spatial, or spectral behavior of the considered biometric. This set is divided into a fixed number of segments according to some randomly selected decomposition key. The transformation function is obtained by performing a linear convolution between the obtained segments. Solving a blind de-convolution problem to extract the original template having no a priori knowledge about the original sequence, is a computationally hard problem.

Yang et al. [112] generated cancelable fingerprint templates by applying non-invertible transforms to Delaunay triangle based local structure of minutiae points rather than individual minutiae points. The method achieves good local structural stability even after distortion, and efficiently preserves the discriminability capability of the transformed template without compromising on non-invertibility.

Pabitha and Latha [65] proposed techniques to generate cancelable retina templates. It generates templates by identifying bifurcation points in blood vessels, which are later subjected to Non-Invertible Construction algorithm (NIC).

Table 2 summarizes the experimental results for various template transformation techniques using biometric salting and non-invertible transforms discussed in this section.

3.3 Multibiometric cancelable systems

Multimodal cancelable schemes were introduced to increase the security, accuracy, and to overcome other limitations of unimodal cancelable biometrics systems. Such systems are capable of using more than one biometric characteristic for verification or identification. In multimodal biometric systems, information fusion is possible at three different levels-feature level, decision level, or score level. Cancelability in multimodal systems is achieved by mixing features and then transforming them (feature level) or transforming each biometric trait separately and combining their matching score (score level). Nanni and Lumini [61] investigated pros and cons of BioHashing technique and suggested a score level fusion of hashed face and fingerprint codes to improve the performance of the system under stolen token scenario. Kanak and Sogukpinar [38] proposed a method which allows a user to be identified by plenty of his features instead of a single one in a revocable fashion. Canuto et al. [16] proposed multibiometric fusion of voice and iris data by subjecting each modality to a combination of three different approaches, BioHashing, Interpolation, and BioConvolving. Each transformed template is trained by an individual classifier and the fusion is performed at the decision level.

Paul and Gavrilova [67] extended cancelable schemes on multimodal biometric systems. Using a feature level fusion scheme and selecting face and ear as the two modalities; the authors proposed a technique that made a two-fold random selection from the feature set of each biometric trait. Random projection method is applied on each fold to achieve cancelability. The authors also proposed multimodal biometric approach to generate cancelable face template based on multi-fold random projection and fuzzy communication. They also presented a random cross folding algorithm to generate multimodal cancelable biometric templates [68]. In their recent work, they suggested a new technique for cancelable fusion of face and ear [69].

Maiorana et al. [53] proposed a multibiometric approach for generating cancelable signature templates. To improve the performance of the system, the technique makes use of BioConvolving to generate cancelable templates which are fused at score level. Recently, Rathgeb and Busch [75] generated cancelable multibiometrics which adapts bloom filter-based transforms to irreversibly mix binary iris templates at the feature level, where iris-codes are obtained from both eyes of a single subject.

3.4 Extending cancelability to cryptosystems

Biometric cryptosystems have the advantage of delivering good recognition rates, but the templates are not revocable. On the other hand, template transformation techniques suffer from the problem of low performance. Both the techniques can be combined appropriately to benefit from each other. Cancelable templates can be generated from cryptosystems by appropriately combing transformations with key-binding and key-generating schemes. This section covers details about works that involve cancelable techniques in combination with existing approaches to generate protected biometric templates. Goh and Ngo [27] generated cancelable face templates using biometric cryptosystems. Their work proposed cryptographic key computations from face templates by BioHashing eigenprojections/face bitmaps. Bringer et al. [9] attempted to improve the performance degradation and loss of discriminability due to irreversible transform. They proposed a technique which applies secure sketches to cancelable biometrics, and completely transforms the original template without compromising the matching performance. Feng et al. [23] proposed a hybrid approach for protecting face template by combining cancelable based transformation techniques with biometric cryptosystems. The scheme consists of a three step hybrid framework based on random projection, class preserving transformation followed by hashing. Later, Feng at al. [24] improved this work and proposed a hybrid algorithm based on random projection, discriminability preserving transform, and fuzzy commitment scheme. Fuzzy vault is a cryptographic framework that binds the biometric template with a cryptographic key. Compromise and cross matching of protected template is possible if an adversary gains access to multiple vaults of a legal user. Feng et al. [22] and Xu et al. [109] proposed cancelable fuzzy vault scheme, which generates different vaults for different cancelable templates. They transformed original template through non-invertible transforms. The transformed template is used to construct the vault. Zhu et al. [113] proposed another hybrid framework which combines random projection and fuzzy vault on voiceprint feature vectors to generate cancelable voiceprint templates. Homomorphic encryption and other schemes cascading cancelable techniques with cryptographic systems are presented in [25, 30, 43]. Table 3 provides details of various hybrid techniques along with their experimental results.

3.5 Possible attacks on various cancelable biometrics approaches

The attacks are aimed at obtaining unauthorized access to some relevant information about the user or his/her original biometric feature from templates in the transformed domain. The key point in the security of a cancelable template is the transformation function design and the transformation parameters associated with it.

- *The Stolen Token Scenario and Pre-Image Attack on BioHashing:* In case of biometric salting techniques, if the user-specific key is compromised then it is possible to reconstruct the original template as the transformations are usually invertible. Since BioHashing is essentially a quantized under-determined linear equation system, it can be solved partially via pseudo-inverse operation. Thus, the performance degrades

Table 3 Some hybrid systems with experimental results

Modality	Author(s)	Database	Technique	FRR/FAR(%)
Face	Feng et al. [23]	CMU	FisherFace	18.18 ERR
			MRP	11.93 ERR
			Cancelable transform + encryption	6.81ERR
Fingerprint	Feng et al. [22]	IBM-GTDB	Fuzzy Vault	79(GAR)/0.21
		FVC2002 DB2	Multiple control Fuzzy Vaults	91(GAR)/0.13
			Cancelable Fuzzy Vaults	92(GAR)/0.21
Fingerprint	Bringer et al. [9]	FVC2000	Secure sketches	5.3 ERR
			Cancelable Secure sketches	1.4 ERR
Voice	Zhu et al. [113]	Mandarin	Original	5.12/0.08
			Multidimensional Fuzzy Vault	5.28/26.43
			Random projecion+Fuzzy Vault	5.12/0.08

severely on stolen token attack. If BioCode and TRN are compromised, inverse operations and pre-image attack can generate a pre-image of original BioCode even without a genuine user's original biometric data [13, 42, 46]. Invertibility is also possible by reverse engineering methods [41]. These computed inverses or pre-images are sufficient for impersonation attacks.

- *The Stolen Token Scenario and Pre-Image Attack on Non-invertible Transforms:* If the knowledge of transformation function and transformation key/parameter is available with the attacker, it is possible for him to approximate the inverse of the transformed template. Attacks has been performed on various non-invertible transforms suggested by Ratha et al. [72] to generate a pre-image template similar to the original templates [58, 71].
- *Attack via Record Multiplicity (ARM):* If multiple transformed templates of the same biometric are available, they can be correlated to retrieve some information or even reconstruct the original template. Success of such attacks depends upon the knowledge of stored templates along with transformation function and parameters [48]. Even though it is computationally infeasible to recover the original biometrics templates from the protected ones, determining whether two protected templates are driven from the same biometric is possible.
- *Privacy and Replay Attacks:* Privacy attacks are passive but a potential threat to the privacy of users, where an attacker tries to locate a user by determining if the same distorted biometric template is being used for a particular transaction. In this case, though the adversary cannot find who is trying to be identified, but can predict whether it is the same person. In the case of replay attacks, the recorded signals can be replayed in a link between sensor and matcher to obtain illegitimate access.
- *Dictionary Attacks:* If two or more transformed templates are available, dictionary attacks make it possible to recover the original biometric template. In such attacks, the attacker simulates the transformation and constructs a set of possible pre-images for each transformed template. Shin et al. [85] presented an algorithm for successfully implementing such attacks on functional transformed based cancelable fingerprint templates.

- *Hill Climbing Attacks:* Such attacks access systems communication channels and match scores. It injects false data into the system and iteratively modifies it till acceptable match score is not generated by the system [55].

3.6 Performance measurement

The performance of a system can be evaluated as *recognition performance* and *protection performance*. To ensure the practical application of cancelable biometrics, recognition performance of the system must be acceptable. Recognition performance of a system is a combination of accuracy, biometric performance, and diversity. FAR and FRR are the metrics that measure accuracy and biometric performance. CMR_T, the Cross Match Rates in the Transformed domain, measures diversity. Table 2 summarizes the experimental results for the various template transformation techniques using biometric salting, non-invertible transform, or their combination with cryptosystems. There exists a trade-off between cancelability and recognition performance. For deployment in real time environments, it is possible to trade some amount of recognition accuracy for providing cancelablity to biometric data. The sensitivity of each transform varies with the choice of the transformation parameters. Various transformation techniques have different impact on the performance [87]. Non-invertible transforms provide better template protection in both signal and feature domain. But they can lead to information loss that affects the discriminating ability of the transformed template (low FAR). As the optimality of feature representation is destroyed by non-invertible transforms, the recognition accuracy deteriorates.

BioHashing projects biometric data on a random subspace such that the pair wise distances of points are similar in some extent before and after the projection. Random projection transforms the vector, but preserves its statistical properties. Hence, the discriminating capability of the feature vector is not lost. BioHashing techniques perform well by preserving intra-class variations and increasing the inter-class variations.

As compared to unimodel systems, Multimodal cancelable biometric systems report a substantial improvement in stolen token scenario. Fusion of multiple biometrics provides more robust and attacks resistant features. An increase in the inter-class variability and performance has been observed in multimodal cancelable systems. Extended cryptosystems combine advantages of both cancelable and cryptographic techniques to provide better template security, intra-class variations, and matching performance.

The overall recognition accuracy and performance of the system depends not only on the transformation functions but also on the registration process, associated parameters, feature extraction, and similarity matching techniques. Since matching is performed in the transformed domain, it is required to have a defined and suitable feature extraction as well as similarity measure techniques in the transformed domain [12]. Diversity is determined by finding the content of mutual information that can be revealed by a set of transformed templates.

Protection performance is irreversibility and unlinkability offered by the transformed template. $IRIS$, the Intrusion Rate due to Inversion for the Same biometric system, and $IRID$, the Intrusion Rate due to Inversion for a Different biometric system, are metrics for irreversibility. BioHashing significantly improves the function performance but it is invertible. Non-invertible transforms claim irreversibility of the transformed template to obtain the original template, yet it is possible to approximate the inverse similar to the original one. To claim irreversibility, the computational complexity to obtain the approximate inverse rather than the exact inverse should be determined. CMR_O, the Cross Match Rates in the Original domain, is measured ensuring unlinkability.

Transforms that keep meaningful relationships with feature extraction and similarity measure needs to be integrated as a whole in any strategy that provides cancelable biometric. Otherwise, the overall performance may not be guaranteed.

3.7 Statistical evaluation and risk assessment

A statistical evaluation of the risks associated with cancelable systems under various attack scenarios is also required. Other than measuring the recognition performance and protection performance, a quantitative measure for robustness of the cancelable systems is also required. Such a framework helps to compare various techniques and assess the risk associated to the feasibility of an attack. Belguechi et al. [3] proposed a framework to evaluate the performance of a cancelable system and its robustness under various attack scenarios. Let b_z and b'_z represent the reference and query template, f be the transformation function, and K_z be the associated transform parameter for a genuine user z. The transformed reference and query template will be $f(b_z, K_z)$ and $f(b'_z, K_z)$, respectively.

3.7.1 Quantify efficiency of a cancelable system

The efficiency of generating accurate matches before and after transformation can be determined as :

$$efficiency = 1 - \frac{AUC(FAR_T, FRR_T)}{AUC(FAR_O, FRR_O)} \tag{1}$$

where AUC represents area under Receiver Operating Characteristics (ROC) curve, FAR_O and FAR_T represent false accept rates in original and transformed domain, and FRR_O and FRR_T represent false reject rates in original and transformed domain respectively. Positive value for *efficiency* denotes increase in performance, while negative value indicates its regression.

3.7.2 Quantify diversity of a cancelable system

Diversity is an essential property of cancelable biometrics that allows generation of multiple different transformed templates of the same user for its use on various applications. The variations are created by changing the transformation key/parameter, or the function itself. However, these transformed templates must not correlate to reveal any information about the original template. To determine if an attacker can obtain any information about the original template, the mutual information content between any two transformed templates X and Y is measured as

$$I(X, Y) = \sum_x \sum_y P(x, y) log \frac{P(x, y)}{P(x)P(y)} \tag{2}$$

where P is the probability estimation. The diversity is measured by computing the mean of the highest value of mutual information for various transformed templates as

$$D = \frac{1}{N} \sum_{i=1}^{N} \sum_{j=1}^{M} max \left(I \left(f \left(b_i^0 \right), f \left(b_i^{j'} \right) \right) \right) \tag{3}$$

where $b_i^{j'}$ denotes the j^{th} test data of i^{th} individual in the database, N is the number of individuals, and M is the number of transformed templates for each individual.

3.7.3 Assessing risk in the case of an attack

Let A_z be the template obtained by the imposter under any attacks scenario. Then, the probability of a successful attack by the impostor is calculated as

$$FAR = P(Distance(f(b_z, K_z), A_z) <= t) \tag{4}$$

where t represents the decision threshold and P is the estimation for probability. High value of FAR implies a high chance for an imposter to gain access. Also, the value can be evaluated for different types of attacks and sorted in the increasing order to determine which attack has high probability for a proposed technique.

3.7.4 Assessing risk associated with revocability

For many applications, the biometric template is revoked by simply changing the transformation key/parameter. It is possible for an attacker to access multiple revoked templates for the same biometric. In such cases there is a risk that by statistical analysis an attacker may predict the most probable values of a new transformed template to be generated. To evaluate the risk, Q number of a transformed templates are generated from the original template by varying the parameter as

$$B = (f(b_z, K_z^1), ..., f(b_z, K_z^Q)) \tag{5}$$

Given these Q transformed templates, a prediction attack can be simulated to evaluate the associated risk by varying the value of Q. This also helps in determining the usability of particular biometric trait and practical number of times it can be revoked without giving up the confidentiality.

3.8 Security and privacy

Cancelable biometrics provides template level security to biometric databases. It meets the specific security requirements of renewability and allows regeneration of templates in case of a compromise. However, it does not defend the system against attacks at points other than the database. Cancelable biometrics can make spoofing all the more difficult as the attacker has to obtain the user-specific token/value along with the biometric samples of the user. Time stamping and dynamic time warping are some approaches which are integrated to transformations for preventing replay attacks. Bringer et al. [10] proposed anonymous identification with cancelable templates using time dependent approach to prevent such attacks.

As the reference template is always made to store in distorted format, they do not reveal the identity of the owner. Often biometric and personal information of a user are linked and subjected to applications beyond those using biometrics. As a consequence, subjects using initial applications are forced to use other applications. Transformed templates are promising against such privacy invasion as it provides unlinkability between biometric templates across various applications. Cancelable templates lose their importance, if the transformed template can be inverted/reversed to approximate or exactly recover the original thus leading to intrusion and linkage attacks.

3.9 Parameters management

As already mentioned, the generation of cancelable templates relies on transforming templates according to some user specific values or parameters. The concept of parameter management is important as the security, privacy, and usability of the system can be compromised if the transformation parameters are handled loosely. A user cannot authenticate in a cancelable system without his transformation parameter. Inverting the transformed template and other attacks possible on various transformation approaches when the parameter is compromised are already discussed in the previous sections. The four models for parameter storage and management are, Store on Client (SOC), Store on Token (SOT), Password based Parameter Management ($PBPG$) model, and Store on Server (SOS) model [95].

SOC model stores parameters on client side authentication devices such as sensors, mobile terminals, or PCs. Each user has a unique ID to which a parameter is linked and stored at authentication device. The user just needs to input his biometric and the transformed template will be automatically generated for matching purposes. The model is very user friendly as there is no need for a user to carry a token or password. However, if there is a compromise for even one of the authentication client, the entire client parameter set needs to be revoked at once. This adds to high operational costs and makes the model unsuitable for applications having very large number of users such as ATMs, POS etc.

In SOT model, the parameter is stored on hardware devices such as USB or smart cards and its management relies entirely on the user. It defines a two factor authentication model where a user needs to provide his/her token in addition to his biometric sample for successful authentication. This model reduces usability as the tokens can be easily lost, stolen, or forgotten at home.

In $PBPG$, the user needs to remember a password which leads to the generation of the transformation parameter. Like SOT, it is also a two factor authentication model which increases security but more user friendly. The generation of password depends on the users' knowledge of the secret which can reduce the possibility of losing token.

In SOS model, there exists a parameter management server which stores the unique ID and transformation parameter for a particular user. At the time of authentication, the user presents his biometric sample and ID, and associated parameter is fetched from the server. Such a model is very user friendly and minimizes risk of losing the parameter. The drawback of this model is that parameter can be disclosed to any authentication client connected to the system. If an authentication client is abused by the attacker the parameter can be easily disclosed.

Any of the four parameter management models discussed here can be used or modified accordingly to meet the needs of an application.

3.10 Cancelable biometrics in the real life applications

TURBINE (Trusted Revocable Biometric Identities) is a 6.3 Million Euro research project funded by the European government for research and technology development. The TURBINE team led by SagemScurit of France is applying cryptographic methods to ensure that the data generated from fingerprints for authentication purposes cannot be used to reconstruct the original fingerprint. In addition, users will be able to create, use, and revoke several "pseudo identities" used for various applications from the same fingerprints [81]. VAST LAB (Vision and Security Technology Lab) by Dr. Terry Boult, University of Colorado, and his company Securics Inc. provide solutions for biometric security based on revocable biometric token (biotoken) [6, 84]. Securics Inc. is exploring the benefits of biotoken for revocable biometric identity solutions. Their unique biotokens are called 'Biotope revocable identity tokens'. The company has commercially made available revocable biotokens for face and fingerprint. The initial commercial function for these biotokens is an authentication application for Web-based transactions. However, the company hopes that the Biotope token would be expandable for use in drivers' licenses and passports.

Priv-ID is an independent company originated from Philips that specializes in providing Privacy Enhancing Technology (PET) for biometric templates. The company offers to generate irreversible binary hash codes from biometric data by applying BioHASH. It is a one way transformation function. The BioHASH matcher is modality independent and works the same for fingerprint, iris, face, or vein information [26]. PerSay is an Israel based company that collaborates with priv-ID to provide voice biometric speaker verification and integrates priv-ID engine to voice biometrics [70].

Hitachi developed a finger vein authentication technology, VeinID. It is a cardless credit payment system, called "finger vein money", which allows shoppers to pay for purchases using only their fingertips. To protect the biometric data in this system, Hitachi used encryption algorithm called Correlation Invariant Image Randomization (CIIR) which matches the encrypted data to an encrypted template without decrypting the data. The storing and authentication performed in encrypted (transformed) domain keeps the biometric data secret from eavesdroppers as well as administrator. Additionally, the encrypted templates can be revoked. If stored data is compromised, it can be canceled and replaced by simply changing the encryption key. Since January 2013, all branch offices of Bank BPH, one of the largest banks in Poland, are using Finger Vein biometrics by Hitachi as a main method of authentication [106]. Precise Biometrics is a Swedish company which offers solutions to secure match-on-card fingerprint verification. The technology can be used for ID, company and bank cards, and for access to mobile solutions, computers, and networks.

4 Visual cryptography (VC)

Naor and Shamir [63] proposed Visual Secret Sharing (VSS) scheme, in which a secret binary image can be cryptographically encoded into n meaningless shares, giving each participant a unique share. The original secret image can be recovered from some or all of these shares by simply stacking them without the need of any complex cryptographic computations. The basic model described by Naor and Shamir was a $k - outof - n$ VSS that encrypts secret image S into n shares $V1$, $V2$, , Vn; where, any k of the n shares are able to reveal the secret, but no combination of $k - 1$ shares can reveal the secret. Figure 6 shows an example of $2 - outof - 2$ VSS on a binary image. Any VSS scheme is characterized by two parameters:

1. *Pixel expansion:* Each pixel of the original image is transformed into n shares, one for each transparency/share image. This involves encoding of a pixel into more than one sub-pixel. The number of sub-pixels required to encode a pixel determines the pixel expansion.
2. *Contrast:* Contrast refers to the quality of the reconstructed image after the decryption.

Performance of VSS is measured by its randomness parameter. Randomness refers to the amount of entropy needed to encode an image. Shannon entropy quantifies the expected value of the information contained in a message.

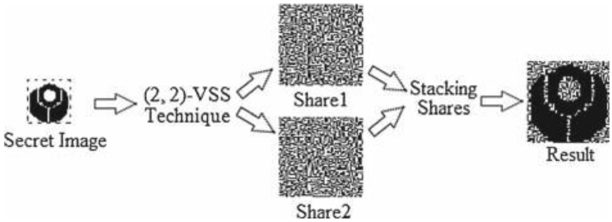


Fig. 6 An exampe of 2-out of-2 VSS [19]

The scheme proposed by Naor and Shamir defines methods to create shares for binary images only. However, new approaches have been proposed that extend to gray-scale and color images too. Biometric template protection using VC schemes have been introduced for various modalities like fingerprint [56], face [79, 80], palmprint [18], and iris [76, 86, 88].

4.1 Visual cryptography for biometric template protection

The data securing techniques provided by VSS are used for covert communication of biometric templates in a distributed format. The biometric template is encrypted into several shares which are distributed amongst the user and database servers. The four biometric template protection criteria as specified by Jain et al. [35] can also be fulfilled with the help of VSS schemes. These are:

1. *Diversity:* For different applications template can be decomposed into different constituting shares, by using different VSS schemes and/or creating different number of shares.
2. *Revocability:* Certain VSS schemes make use of some predefined or randomly selected auxiliary data (such as cover images or host images) while generating shares. These shares can be suspended or replaced time to time to generate revocable template. Not all schemes can be applied to achieve revocability. The contention of producing revocable templates using VSS is a challenge to be met.
3. *Security:*It is computationally hard to obtain the secret image by any individual share or shares less than the required number. Also, by storing the shares on a distributed server, the chances of obtaining the secret image is minimized. Data stored on the distributed server prevents unauthorized modification and inaccurate updates.
4. *Performance:* The performance of recognition systems does not degrade when the original biometric template is reconstructed from its constituting shares using various VSS approaches if the contrast (quality) is optimally preserved while reconstructing.

The underlying operation of the VC schemes as proposed by Naor and Shamir uses Boolean OR operation while stacking the shares to reconstruct the secret image. XOR based VC schemes define a similar model for generating secret shares in which the Boolean XOR is used as the underlying operator. For any OR based VSS the minimum pixel expansion is 2, whereas for any XOR based VSS there may be no pixel expansion. Tuyls et al. [103] provided details on creating shares using XOR based VC schemes. Monoth and Babu [56] utilized a simple XOR based secret sharing technique for fingerprint images to prevent tampering, and securing their storage and transmission over the network. Based on the existing framework, Ilavarsan and Malvika [33] proposed a multiple level VC scheme for securing templates without pixel expansion.

Existing VC techniques encrypt an image into n meaningless shares which appear like a random noise. Such shares tend to arouse the curiosity of an adversary by suggesting the presence of some hidden information in random noise like patterns. Extended Visual Cryptography (EVC) scheme is a framework proposed by Ateniese et al. [2]. Instead of producing noise like shares, EVC reformulates shares as natural images. This mitigates the concern of the adversary for the idea of the presence of some secret information. To apply the same framework on gray-level images, Nakajima and Yamaguchi [59] proposed Gray level Extended Visual Cryptography Scheme (GEVCS) and also introduced a method to enhance the contrast of the target images. GEVCS transforms gray-level images into meaningful binary images (also known as halftone images) by changing the dynamic range of the original and host images. Ross and Othman [80] proposed a technique based on GEVCS to encrypt an individuals face image into two independent public host images (natural images) to deceive the adversary. The encrypted shares look like a natural face and not random noise. The host images which are used to hide the secret image are previously made to store in a public dataset. The original face image can be reconstructed only when both the public images are available. Figure 7 illustrates an example of this approach. In case of a compromise, the existing shares are revoked and new shares can be created easily by changing the host images. Using the similar techniques, Ross and Othman [64, 78] provided techniques for de-identifying fingerprints and iris codes before storing them on a central database. The techniques provided by Ross and Othman were successful in providing revocability to the biometric templates.

Revenker et al. [76] proposed techniques for securing iris feature template. The method requires a secret binary image (to be chosen by the system administrator) as an input to the visual cryptography algorithm along with the iris code, to generate the secret shares. By changing the secret binary image, different sets of shares can be generated for the same iris template. Scrambling the original biometric data by random permutations before subject it to VC paves ways to enhance the security of the template. Muhammed [57] suggested a

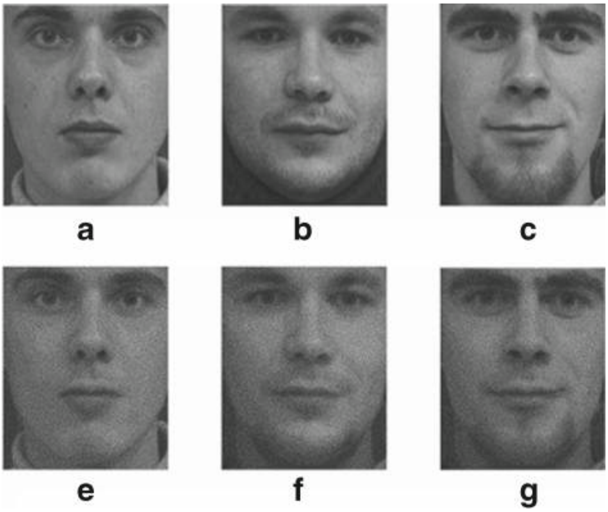


Fig. 7 Encryption of a private face image in two prealigned and cropped face images. **a** and **b** are two host images, **c** is a private face image. **e** and **f** are the host images after visual encryption (two sheets). **g** is the result of overlaying **e** and **f** [19]

technique which performs random block permutations on the template and creates shares out of it by applying VC. In case of compromise, new shares can be created by changing the permutation.

Recursive Visual Cryptography (RVC) allows recursive creation of shares and embeds secret into shares using basic schemes. Takur et al. [96] proposed a technique to secure biometric data using RVC. The shares are created by using multiple resolution VC schemes which allow smaller secret to be hidden within one large share in recursive manner.

4.2 Visual cryptography and biometric cryptosystems

In biometric cryptosystems protected version of a biometric template is created by binding a key with the original template. Like the proposed VSS schemes, cryptosystems require the exact biometric template to be recovered while performing authentication. However unlike the cryptosystems, there is no key association required in VSS. The decryption process relies entirely on the availability of the encrypted shares to recover the secret. Fuzzy vault is based on the same basic principle as that of visual cryptography, i.e., secret sharing. In fuzzy vaults scheme a feature vector is represented as a polynomial of degree k and encoded as a set of n points, where $k + 1 < n$. To unlock the vault a set of $k + 1$ valid points are required, which are interpolated using Lagrange's interpolation to recover the polynomial of degree k. This derives an analogy to VSS schemes, which also defines a secret to be shared into a set of n shares, such that any $k - outof - n$ shares, $(k \leq n)$ can recover the secret. Both the approaches offer order invariance property, implying that the sets/shares need to recover the secret need not to be acquired in a defined order.

4.3 Possible attacks on visual cryptography schemes

Visual cryptography secures biometric template at database level which decomposes image template into shares and distributes amongst participants. There are two types of participants in VC. The authorized participants are known as qualified participants, and the unauthorized participants are known as outsiders. When these two types of participants are involved in abusing the system, the qualified participants are known as malicious participants, and outsiders are known as malicious outsiders [32].

A Malicious Participant (MP) generates a fake share with the help of his original share and tries to cheat genuine users. As the fake share seems indistinguishable from the original, the other genuine users lend their shares. The resultant image (fake secret image) created from overlapping the fake share and the other genuine shares would be different from the original secret image. But the genuine users are cheated to believe that the fake secret image is the original secret image.

Malicious Outsider (MO) is the participant who is not in possession of any genuine share of the image. Malicious outsider tries to cheat by creating a random fake share of size equal to the size of the genuine shares. As the size of the secret shares is not known to him, he tries to tune the size of the fake share to stack it with the genuine share. Another possible attack is the cheating of EVCS by MP. The idea is to use the fake shares to reduce the contrast between the share images and the background. Simultaneously, the fake image in the stacking of fake shares has enough contrast against the background since the fake image is recovered in the perfect blackness.

Such attacks can lead to intrinsic failure or denial-of-service (DoS) which renders the system unavailable to its intended users.

4.4 Security and privacy

Visual cryptography approaches provide security to the system against database attacks by never storing the reference template in a clear format and can assist in their recovery in case of loss or compromise (revocability). The approaches allow shares to be provided to the user in a tokenized format thus weakening possibilities of spoofing attacks. The approaches can be modeled appropriately to address other attacks such as man-in-middle attacks as the computation at user/matcher site may be dependent on shares which are never transferred over a network. The approaches can resist invertibility attacks on stored template database until and unless all the required number of shares (some of them may be stored with user and some at other storage locations) are available to the attacker. The existing works makes use of auxiliary data, such as cover images to improvise privacy by enabling covert communications and address the issue of cross-linkability.

4.5 Performance measurement

Pixel expansion, accuracy, and computational complexity are measured for evaluating *recognition performance*. The major limitation of conventional VC schemes is the increase in size of shares due to pixel expansion, which directly leads to an increase in storage space and cost. Accuracy depends on the quality of the reconstructed secret image and evaluated by Peak Signal-to-Noise Ratio (PSNR). Many VSS schemes have been suggested in literature that allows creating lossless shares under optimal pixel expansion. The Gray-level Extended Visual Cryptography Scheme (GEVCS) for creating natural looking shares requires cost of registering (aligning) each public image with the private image. In case of improper registration, the quality of the generated shares and the reconstructed image can degrade. Computational complexity depends upon the number of operations required to generate the shares and reconstruct original image from it.

Protection performance depends upon the security of shares and unlinkability. Security is satisfied if any information about the secret image is not revealed by any individual shares or shares less than the required number. Unlinkability requires no correlation to exist between shares created for the same biometric across various applications.

Distributed storage of the shares also leads to increase in storage costs. Registration and storage have to be optimized in order to maintain the recognition performance and the cost of biometric systems.

5 Conclusion

Cancelable biometrics and visual cryptography schemes successfully fulfills the criteria for biometric template protection. These schemes enhance privacy of the template while storing and transmission and also provides high level security to the biometric authentication systems. Described approaches operate on the transformed template without any potential drop in the recognition rates and performance. As both the schemes operate in the transformed domain, some of the privacy concerns like searching or cross matching of legacy database are alleviated. The major issue that often results to low recognition rates in both the schemes is the issue of registration. The schemes have to incur extra cost while registering/aligning the transformed sample. The review includes the sections that discuss the vulnerability of the systems against possible attacks and defensive measures that can be taken to avoid them.

Cancelable biometrics has been a revolution in technology as it allows to generate revocable biometric identities which are difficult to be forged and can be generated innumerable times for the same user. The scheme distorts the original biometric with the help of some non-invertible transforms, or salting. It enhances privacy as different transforms are used for different services and applications, and true biometrics is never revealed while storing or matching. Revocation is possible by changing the distortion parameters and/or distortion function. Some of the approaches involving salting techniques have been reported to increase in functional performance of the system. Design of non-invertible functions require maintaining a balance between discriminability and invertibility for optimizing the performance of the recognition systems. The discussed hybrid approaches take advantage of different schemes to provide improved performance. Commercial deployments and implementations of these approaches have been cited where ever possible.

Visual cryptography is an emerging secret sharing scheme deployed on images. The contribution of the scheme for securing biometric templates is examined. VC approaches allow the sample to be encrypted in several secret shares, which are saved on distributed storage systems such that, each individual share does not reveal any information about the original sample. The scheme enhances the privacy of the stored biometric as it is not stored in a centralized database in the original format, but on distributed database in encrypted format. For different applications different cryptography schemes can be utilized to prevent linking and cross matching of databases. In addition to security, diversity, and performance, several VC approaches can also provide revocability to the biometric template as discussed. The scheme allows only the verification of biometric identity, where the input sample is made to match with the stored sample of the same person and not with all the stored samples. Only a few applications have been proposed that implement the scheme [92], as the proposed scheme is not matured enough for deployments in commercial applications involving biometric based recognition. A rigorous analysis of the vulnerabilities and attacks is required to be done before deploying it on the large scale, either commercial or the real world applications.

References

1. Ang R, Safavi-Naini R, McAven L (2005) Cancelable key-based fingerprint templates. In: Information Security and Privacy. Springer, pp 242–252
2. Ateniese G, Blundo C, Santis AD, Stinson DR (2001) Extended capabilities for visual cryptography. Theor Comput Sci 250(1):143–161
3. Belguechi R, Cherrier E, El Abed M, Rosenberger C (2011) Evaluation of cancelable biometric systems: Application to finger-knuckle-prints. In: 2011 International Conference on Hand-Based Biometrics (ICHB). IEEE, pp 1–6
4. Belguechi R, Cherrier E, Rosenberger C (2012) Texture based fingerprint biohashing: Attacks and robustness. In: 2012 5th IAPR International Conference on Biometrics (ICB). IEEE, pp 196–201
5. Bolle RM, Connell JH, Ratha NK (2002) Biometric perils and patches. Pattern Recog 35(12):2727–2738
6. Boult T Vision and Security Technology Lab. http://www.vast.uccs.edu
7. Boult TE, Scheirer WJ, Woodworth R (2007) Revocable fingerprint biotokens: Accuracy and security analysis. In: 2007 IEEE Conference on Computer Vision and Pattern Recognition, CVPR'07. IEEE, pp 1–8
8. Bringer J, Chabanne H, Cohen G, Kindarji B, Zémor G (2007) Optimal iris fuzzy sketches. In: First IEEE international conference on biometrics: theory, applications, and systems, 2007. BTAS 2007. IEEE, pp 1–6
9. Bringer J, Chabanne H, Kindarji B (2008) The best of both worlds: Applying secure sketches to cancelable biometrics. Sci Comput Program 74(1):43–51

10. Bringer J, Chabanne H, Kindarji B (2009) Anonymous identification with cancelable biometrics. In: Proceedings of 6th International Symposium on Image and Signal Processing and Analysis, ISPA 2009. IEEE, pp 494–499
11. Chen X, Bai X, Tao X, Pan X (2013) Chaotic random projection for cancelable biometric key generation. In: Intelligent Science and Intelligent Data Engineering. Springer, pp 605–612
12. Cheung KH, Kong A, Zhang D, Kamel M, You JT, Lam HW (2005a) An analysis on accuracy of cancelable biometrics based on biohashing. In: Knowledge-Based Intelligent Information and Engineering Systems. Springer, pp 1168–1172
13. Cheung KH, Kong AWK, You J, Zhang D (2005b) An analysis on invertibility of cancelable biometrics based on biohashing. In: CISST, vol 2005, pp 40–45
14. Clancy TC, Kiyavash N, Lin DJ (2003) Secure smartcard based fingerprint authentication. In: Proceedings of the 2003 ACM SIGMM workshop on biometrics methods and applications. ACM, pp 45–52
15. Connie T, Teoh A, Goh M, Ngo D (2005) Palmhashing: a novel approach for cancelable biometrics. Inf Process Lett 93(1):1–5
16. de Paula Canuto AM, Fairhurst MC, Pintro F (2013) Ensemble systems and cancellable transformations for multibiometric-based identification. IET Biom 3(1):29–40
17. Dey N, Nandi B, Dey M, Biswas D, Das A, Chaudhuri SS (2013) Biohash code generation from electrocardiogram features. In: 2013 IEEE 3rd International Advance Computing Conference (IACC). IEEE, pp 732–735
18. Divya C, Surya E (2012) Visual cryptography using palm print based on dct algorithm. International Journal of Emerging Technology and Advanced Engineering 2(12):2250–2459
19. Fan TY, Chieu BC, Chao HC (2012) Robust copyright-protection scheme based on visual secret sharing and bose–chaudhuri–hocquenghem code techniques. Journal of Electronic Imaging 21(4):043,018–043,018
20. Farooq F, Bolle RM, Jea TY, Ratha N (2007) Anonymous and revocable fingerprint recognition. In: 2007 IEEE Conference on Computer Vision and Pattern Recognition, CVPR'07. IEEE, pp 1–7
21. Feng H, Choong Wah C (2002) Private key generation from on-line handwritten signatures. Inf Manag Comput Secur 10(4):159–164
22. Feng Q, Xiao Y, Su F, An CAI (2008) Cancelable fingerprint fuzzy vault scheme. J Comput Appl 7: 060
23. Feng Y, Yuen PC, Jain AK (2008) A hybrid approach for face template protection. In: SPIE Defense and Security Symposium, International Society for Optics and Photonics, pp 694,408–694,408
24. Feng YC, Yuen PC, Jain AK (2010) A hybrid approach for generating secure and discriminating face template. IEEE Transactions on Information Forensics and Security 5(1):103–117
25. Gaddam SV, Lal M (2010) Efficient cancelable biometric key generation scheme for cryptography. IJ Netw. Secur 11(2):61–69
26. Genkey. http://www.priv-id.com
27. Goh A, Ngo DC (2003) Computation of cryptographic keys from face biometrics. In: Communications and Multimedia Security. Advanced Techniques for Network and Data Protection. Springer, pp 1–13
28. Hämmerle-Uhl J, Pschernig E, Uhl A (2009) Cancelable iris biometrics using block re-mapping and image warping. In: Information Security. Springer, pp 135–142
29. Hao F, Anderson R, Daugman J (2006) Combining crypto with biometrics effectively. IEEE Trans Comput 55(9):1081–1088. IEEE
30. Hirano T, Hattori M, Ito T, Matsuda N, Mori T (2012) Homomorphic encryption based cancelable biometrics secure against replay and its related attack. In: 2012 International Symposium on Information Theory and its Applications (ISITA), IEEE, pp 421–425
31. Hirata S, Takahashi K (2009) Cancelable biometrics with perfect secrecy for correlation-based matching. Springer, pp 868–878
32. Hu CM, Tzeng WG (2007) Cheating prevention in visual cryptography. IEEE Trans Image Process 16(1):36–45
33. Ilavarsan K, Malvika R (2012) A multiple level visual cryptography scheme for biometric privacy without pixel expansion. International Journal of Communications and Engineering 4(4):59–63
34. Jain AK, Ross A, Prabhakar S (2004) An introduction to biometric recognition. IEEE 14:4–20
35. Jain AK, Nandakumar K, Nagar A, et al. (2008) Biometric template security. EURASIP Journal on Advances in Signal Processing 2008
36. Jeong M, Lee C, Kim J, Choi JY, Toh KA, Kim J (2006) Changeable biometrics for appearance based face recognition. In: 2006 Biometrics Symposium: Special Session on Research at the Biometric Consortium Conference. IEEE, pp 1–5

37. Juels A, Wattenberg M (1999) A fuzzy commitment scheme. In: Proceedings of the 6th ACM conference on Computer and communications security. ACM, pp 28–36
38. Kanak A, Sogukpınar I (2009) Classification based revocable biometric identity code generation. In: Biometric ID Management and Multimodal Communication. Springer, pp 276–284
39. Kim Y, Toh KA (2007) A method to enhance face biometric security. In: Biometrics: 2007 First IEEE International Conference on Theory, Applications, and Systems, BTAS 2007. IEEE, pp 1–6
40. Kuan YW, Teoh AB, Ngo DC (2007) Secure hashing of dynamic hand signatures using wavelet-fourier compression with biophasor mixing and 2 n discretization. EURASIP Journal on Applied Signal Processing 2007(1):32–32
41. Kümmel K, Vielhauer C (2010) Reverse-engineer methods on a biometric hash algorithm for dynamic handwriting. In: Proceedings of the 12th ACM workshop on Multimedia and security. ACM, pp 67–72
42. Lacharme P, Cherrier E, Rosenberger C, et al. (2013) Preimage attack on biohashing. In: International Conference on Security and Cryptography (SECRYPT)
43. Lalithamani N, Soman S (2009) An efficient approach for non-invertible cryptographic key generation from cancelable fingerprint biometrics. In: 2009 International Conference on Advances in Recent Technologies in Communication and Computing, ARTCom'09. IEEE, pp 47–52
44. Lee C, Kim J (2010) Cancelable fingerprint templates using minutiae-based bit-strings. J Netw Comput Appl 33(3):236–246
45. Lee Y, Lee Y, Chung Y, Moon K (2007) One-time templates for face authentication. In: 2007 International Conference on Convergence Information Technology. IEEE, pp 1818–1823
46. Lee Y, Chung Y, Moon K (2009) Inverse operation and preimage attack on biohashing. In: Computational Intelligence in Biometrics: 2009 IEEE Workshop on Theory, Algorithms, and Applications, CIB 2009. IEEE, pp 92–97
47. Leng L, Zhang J, Khan M, Bi X, Ji M (2010) Cancelable palmcode generated from randomized gabor filters for palmprint protection. In: 2010 25th International Conference of Image and Vision Computing New Zealand (IVCNZ). IEEE, pp 1–6
48. Li C, Hu J (2013) Attacks via record multiplicity on cancelable biometrics templates. Concurrency and Computation: Practice and Experience
49. Li H, Wang L (2012) Chaos-based cancelable palmprint authentication system. Procedia Engineering 29(0):1239–1245
50. Li Q, Chang EC (2006) Robust, short and sensitive authentication tags using secure sketch. In: Proceedings of the 8th workshop on Multimedia and security. ACM, pp 56–61
51. Lumini A, Nanni L (2007) An improved biohashing for human authentication. Pattern Recognit 40(3):1057–1065
52. Maiorana E, Campisi P, Fierrez J, Ortega-Garcia J, Neri A (2010) Cancelable templates for sequence-based biometrics with application to on-line signature recognition. IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans 40(3):525–538
53. Maiorana E, Campisi P, Neri A (2011a) Bioconvolving: Cancelable templates for a multi-biometrics signature recognition system. In: 2011 IEEE International Systems Conference (SysCon). IEEE, pp 495–500
54. Maiorana E, Campisi P, Neri A (2011b) Cancellable biometrics for on-line signature recognition. New Technologies for Digital Crime and Forensics: Devices, Applications, and Software, p 290
55. Martinez-Diaz M, Fierrez-Aguilar J, Alonso-Fernandez F, Ortega-Garcia J, Siguenza J (2006) Hill-climbing and brute-force attacks on biometric systems: A case study in match-on-card fingerprint verification. In: Proceedings 2006 40th Annual IEEE International Carnahan Conferences Security Technology. IEEE, pp 151–159
56. Monoth T, Anto PB (2010) Tamperproof transmission of fingerprints using visual cryptography schemes. Procedia Computer Science 2:143–148
57. Muhammed RP (2011) A secured approach to visual cryptographic biometric template. International Journal on Information Technology 1(2)
58. Nagar A, Jain AK (2009) On the security of non-invertible fingerprint template transforms. IEEE, pp 81–85
59. Nakajima M, Yamaguchi Y (2002) Extended visual cryptography for natural images
60. Nandakumar K, Jain AK, Pankanti S (2007) Fingerprint-based fuzzy vault: Implementation and performance. IEEE Transactions on Information Forensics and Security 2(4):744–757
61. Nanni L, Lumini A (2006) Empirical tests on biohashing. Neurocomputing 69(16):2390–2395
62. Nanni L, Lumini A (2010) Cancellable biometrics: problems and solutions for improving accuracy. Biometrics: Methods, Applications and Analyses
63. Naor M, Shamir A (1995) Visual cryptography. In: Advances in CryptologyEUROCRYPT'94. Springer, pp 1–12

64. Othman A, Ross A (2011) Mixing fingerprints for generating virtual identities. In: 2011 IEEE International Workshop on Information Forensics and Security (WIFS). IEEE, pp 1–6
65. Pabitha M, Latha L (2013) Efficient approach for retinal biometric template security and person authentication using noninvertible constructions. Int J Comput Appl 69(4)
66. Patel VM, Chellappa R, Tistarelli M (2010) Sparse representations and random projections for robust and cancelable biometrics. In: 2010 11th International Conference on Control Automation Robotics & Vision (ICARCV). IEEE, pp 1–6
67. Paul PP, Gavrilova M (2012a) Multimodal biometric approach for cancelable face template generation. In: SPIE Defense, Security, and Sensing, International Society for Optics and Photonics, pp 84,070H–84,070H
68. Paul PP, Gavrilova ML (2012b) A novel cross folding algorithm for multimodal cancelable biometrics. International Journal of Software Science and Computational Intelligence (IJSSCI) 4(3):20–37
69. Paul PP, Gavrilova M, Klimenko S (2013) Situation awareness of cancelable biometric system. Vis Comput:1–9
70. Persay. http://www.persay.com
71. Quan F, Fei S, Anni C, Feifei Z (2008) Cracking cancelable fingerprint template of ratha. In: 2008 International Symposium on Computer Science and Computational Technology, ISCSCT'08, vol 2. IEEE, pp 572–575
72. Ratha N, Connell J, Bolle RM, Chikkerur S (2006) Cancelable biometrics: A case study in fingerprints. In: 2006 18th International Conference on Pattern Recognition, ICPR 2006, vol 4. IEEE, pp 370–373
73. Ratha NK, Connell JH, Bolle RM (2001) Enhancing security and privacy in biometrics-based authentication systems. IBM Syst J 40(3):614–634
74. Ratha NK, Chikkerur S, Connell JH, Bolle RM (2007) Generating cancelable fingerprint templates. IEEE Transactions on Pattern Analysis and Machine Intelligence 29(4):561–572
75. Rathgeb C, Busch C (2014) Cancelable multi-biometrics: Mixing iris-codes based on adaptive bloom filters. Computers & Security
76. Revenkar P, Anjum A, Gandhare W (2010) Secure iris authentication using visual cryptography. arXiv preprint arXiv:10041748
77. Roberts C (2007) Biometric attack vectors and defences. Computers & Security 26(1):14–25
78. Ross A, Othman A (2011a) Mixing fingerprints for template security and privacy. In: Proceedings of the 19th Eur. Sign. Proc. Conf.(EUSIPCO)
79. Ross A, Othman A (2011b) Visual cryptography for biometric privacy. IEEE transactions on information forensics and security 6(1):70–81
80. Ross A, Othman AA (2010) Visual cryptography for face privacy. In: SPIE Defense, Security, and Sensing, International Society for Optics and Photonics, pp 76,670B–76,670B
81. Rust C (2009) Turbine: Trusted revocable biometric identities. Biometric Technology Today 17(2):8–10
82. Savvides M, Kumar BV, Khosla PK (2004) Cancelable biometric filters for face recognition. In: 2004 Proceedings of the 17th International Conference on Pattern Recognition, ICPR 2004, vol 3. IEEE, pp 922–925
83. Schneier B (1999) Biometrics: uses and abuses. Commun ACM 42(8):58
84. SECURICS INC Colorado springs, co. http://www.securics.com
85. Shin SW, Lee MK, Moon D, Moon K (2009) Dictionary attack on functional transform-based cancelable fingerprint templates. ETRI j 31(5)
86. Siew Chin C, Beng Jin AT, Chek Ling DN (2006) High security iris verification system based on random secret integration. Comp Vision Image Underst 102(2):169–177
87. Simoens K, Yang B, Zhou X, Beato F, Busch C, Newton EM, Preneel B (2012) Criteria towards metrics for benchmarking template protection algorithms. In: 2012 5th IAPR International Conference on Biometrics (ICB). IEEE, pp 498–505
88. Sinduja R, Sathiya R, Vaithiyanathan V (2012) Sheltered iris attestation by means of visual cryptography (sia-vc). In: 2012 International Conference on Advances in Engineering, Science and Management (ICAESM), pp 650–655
89. Sohn H, Ro YM, Plataniotis KN (2009) Biometric authentication using augmented face and random projection. In: 2009 Biometrics: IEEE 3rd International Conference on Theory, Applications, and Systems BTAS'09. IEEE, pp 1–6
90. Soutar C, Roberge D, Stoianov A, Gilroy R, Kumar BV (1998) Biometric encryption using image processing. In: Photonics West'98 Electronic Imaging, International Society for Optics and Photonics, pp 178–188
91. Soutar C et al (2002) Biometric system security. White Paper, Bioscrypt, http://www.bioscrypt.com

92. Suryadevara S, Naaz R, Kapoor S, Sharma A, et al. (2011) Visual cryptography improvises the security of tongue as a biometric in banking system. In: 2011 2nd International Conference on Computer and Communication Technology (ICCCT). IEEE, pp 412–415
93. Sutcu Y, Sencar HT, Memon N (2005) A secure biometric authentication scheme based on robust hashing. In: Proceedings of the 7th workshop on Multimedia and security. ACM, pp 111–116
94. Sutcu Y, Li Q, Memon N (2007) Protecting biometric templates with sketch: Theory and practice. IEEE Transactions on Information Forensics and Security 2(3):503–512
95. Takahashi K, Hirata S (2011) Parameter management schemes for cancelable biometrics. In: 2011 IEEE Workshop on Computational Intelligence in Biometrics and Identity Management (CIBIM). IEEE, pp 145–151
96. Takur V, Jaiswal R, Sonawane S, Nalavade R, et al. (2012) Biometric data security using recursive visual cryptography. In: Information and Knowledge Management, vol 2, pp 32–36
97. Teoh ABJ, Ngo DCL (2006) Biophasor: Token supplemented cancellable biometrics. In: 2006 9th International Conference on Control, Automation, Robotics and Vision, ICARCV'06. IEEE, pp 1–5
98. Teoh A, Yuang CT (2007) Cancelable biometrics realization with multispace random projections. IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics 37(5):1096–1106
99. Teoh AB, Kuan YW, Lee S (2008) Cancellable biometrics and annotations on biohash. Pattern Recog 41(6):2034–2044
100. Teoh ABJ, Ngo DCL, Goh A (2004) Biohashing: two factor authentication featuring fingerprint data and tokenised random number. Pattern Recog 37(11):2245–2255
101. Teoh A, Jin B, Connie T, Ngo D, Ling C (2006) Remarks on biohash and its mathematical foundation. Inf Process Lett 100(4):145–150
102. Tulyakov S, Farooq F, Govindaraju V (2005) Symmetric hash functions for fingerprint minutiae. In: Pattern Recognition and Image Analysis. Springer, pp 30–38
103. Tuyls P, Hollmann HD, Van Lint JH, Tolhuizen L (2005) Xor-based visual cryptography schemes. Des Codes Crypt 37(1):169–186
104. Uludag U, Pankanti S, Prabhakar S, Jain AK (2004) Biometric cryptosystems: issues and challenges. Proc IEEE 92(6):948–960
105. Vielhauer C, Steinmetz R, Mayerhöfer A (2002) Biometric hash based on statistical features of online signatures. In: Proceedings of the 16th international conference on pattern recognition, 2002, vol 1. IEEE, pp 123–126
106. VeinID Hitachi. http://www.hitachi.eu
107. Wang Y, Plataniotis K (2007) Face based biometric authentication with changeable and privacy preservable templates. In: 2007 Biometrics Symposium. IEEE, pp 1–6
108. Wu X, Qi N, Wang K, Zhang D (2008) An iris cryptosystem for information security. In: IIHMSP'08 international conference on intelligent information hiding and multimedia signal processing, 2008. IEEE, pp 1533–1536
109. Xu D, Wang X (2010) A scheme for cancelable fingerprint fuzzy vault based on chaotic sequence. In: 2010 International Conference on Mechatronics and Automation (ICMA). IEEE, pp 329–332
110. Xu W, Cheng M (2008) Cancelable voiceprint template based on chaff-points-mixture method. In: Proceedings of the 2008 International Conference on Computational Intelligence and Security-Volume 02, IEEE Computer Society, pp 263–266
111. Xu W, He Q, Li Y, Li T (2008) Cancelable voiceprint templates based on knowledge signatures. In: 2008 International Symposium on Electronic Commerce and Security. IEEE, pp 412–415
112. Yang W, Hu J, Wang S, Yang J (2013) Cancelable fingerprint templates with delaunay triangle-based local structures. In: Cyberspace Safety and Security. Springer, pp 81–91
113. Zhu HH, He QH, Li YX (2012) A two -step hybrid approach for voiceprint-biometric template protection. In: 2012 International Conference on Machine Learning and Cybernetics (ICMLC), vol 2, pp 560–565. doi:10.1109/ICMLC.2012.6358984
114. Zuo J, Ratha NK, Connell JH (2008) Cancelable iris biometric. In: 2008 19th International Conference on Pattern Recognition, ICPR 2008. IEEE, pp 1–4

Harkeerat Kaur received B.E degree from JEC, Jabalpur (2012). Presently, she is pursuing Ph.D. in Computer Science & Engineering from PDPM Indian Institute of Information Technology, Design & Manufacturing (IIITDM) Jabalpur, India. Her research interests include computer vision, image processing, biometrics and visual cryptography.

Pritee Khanna holds master degrees in Physics as well as in Computer Applications from Kanpur University and Kurukshetra University, India, respectively. She received her doctoral degree in 2004. Presently, she is an Associate Professor in Computer Science & Engineering at Indian Institute of Information Technology, Design and Manufacturing Jabalpur, India. She has published over 45 research papers in journals and conferences of repute. Her research interests include human-computer interaction, content based image retrieval, and biometrics.