Crypto-Biometric Systems as a Framework against Spoofing Attacks

Sukhchain Kaur[1], Reecha Sharma[2]

[1,2]*Department of Electronics and Communication,Punjabi university Patiala,India*

Abstract-*Biometric systems like any security system is exposed to mischievous attackers, who can mold data to make system abortive by implicating its probity. Current theory and design methods of biometric systems do not consider vulnerability of such adversary attacks. In order to make biometric systems secure it is requisite to understand and evaluate the threats and thus to develop adequate countermeasures and robust system designs. Among all the potential attacks, spoof attacks and attacks on template are one of the main threats against the security of biometric systems. In this paper, detection, encryption and anti-spoofing measures have been proposed to deal with these threats. Multimodal biometric systems are intrinsically more robust to spoof attacks than systems based on a single biometric trait, as they combine information coming from different biometric traits. Further liveness detection is carried out to ensure the security in multimodal biometric systems and crypto-biometric system is developed to reduce the risk of exposure of the combined template, if a single trait revealed to simultaneously make system privacy friendly.*

Keywords- *Biometrics, cryptography, cryptosystems, spoofing, template protection, security, spoofing countermeasures.*

I INTRODUCTION

Biometric authentication systems offer several advantages over traditional authentication systems such as Id cards and passwords. As here, they make use of our own behavioural and psychological characteristics to provide authentication systems that guarantee non-repudiation [1]. Biometric information cannot be acquired by direct covert observation. It is impossible to share and difficult to reproduce. In spite of numerous advantages biometric systems are vulnerable to attacks that decrease the security of the system. Adversary attacks involve system's vulnerability at more than one interfaces. Fig 1 below shows a graphical diagram of the attacks in biometric systems where security of the system can be compromised [2].

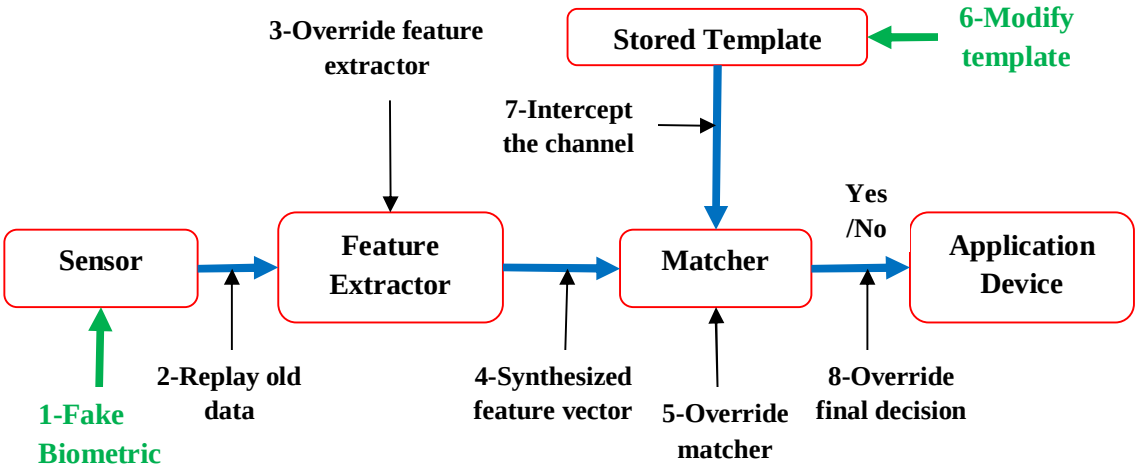

Figure 1: Graphical Representation of possible Attacks on Biometric System.

Type 1 attack include presenting fake samples of person's biometric trait or tries to gain benefit from the leakage of stored information in the database to circumvent the system.

Type 2 attack occurs between scanner and feature extractor. When scanner module acquires given biometric traits and send it to feature extractor then attacker may replay old data to feature extractor bypassing the sensor.
Type 3 attack occurs on the feature extraction module where the feature extractor is attacked using a Trojan horse so that it produces feature sets chosen by the intruder.
Type 4 attack occurs on channel between feature extractor and matcher which includes replacing legitimate feature sets extracted from the biometric module with synthetic feature sets.
Type 5 attack occurs on matcher and it includes corrupting the matcher so that it produces preselected match scores.
Type 6 attack occurs on template database where attacker can modify existing templates, add new templates and delete templates.
Type 7 attack intercepts the communication channel between the database and matcher where the data sent to the matcher through a communication channel are modified before they reached the matcher.
Type 8 attack occurs on channel between the matcher and application where output by the biometric system may be overridden with the choice of result from the attacker.

Among all the above attacks feasibility of TYPE 1 attack also known as “spoof attack” is much higher than other types of attacks against biometric systems, as it does not require any knowledge on the system, such as the feature extraction or matching algorithm used.

Further, a physical spoof of biometric trait can be created by gaining access to the biometric database. In such a condition, reconstruction of original template along with its raw usage or synthesization of fake biometric traits is severely complicated which leads to the fact that “attack on template database” i.e. TYPE 6 attack act as a straightway reason for decreasing the security of the system. This dependency of template attacks against spoof attacks can be shown with greater transparency in the following diagram.

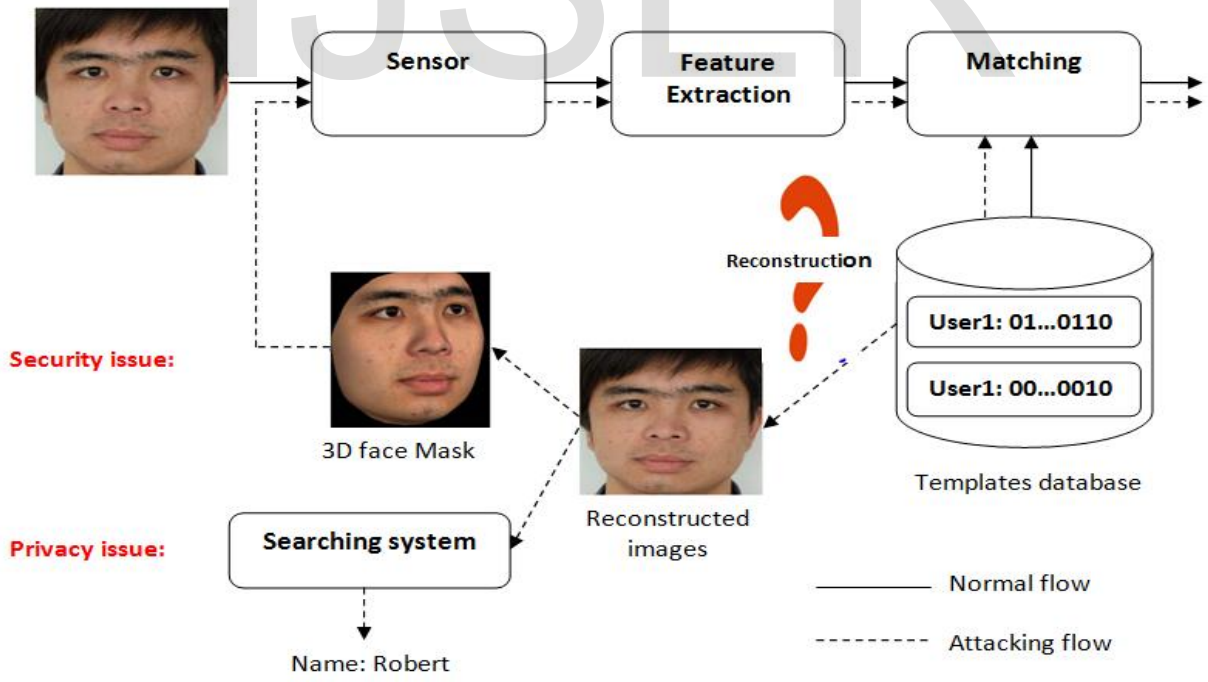

Figure 2: Spoof attack using stolen template database.

II RELATED WORK

Technologies employing single or multi-biometric crypto-biometric systems have been encountered to prevent from spiteful performances, while stay unprotected to classic spoofing ones [3]. For increasing robustness in multimodal biometric systems, combination of uncorrelated modalities such as face and fingerprint is needed rather than using multiple samples of same biometric trait such as multiple fingers of same person. Also, design of stronger fusion rules (score level or feature level) between samples is required [4]. In case of spoof detection, the main objective is to provide protected environment to the system which can accept genuine users and prevent impostor user's to circumvent the system [5]. One of the most robust techniques for the detection and prevention from spoofing attacks is liveness detection which involves processing of additional discriminating features extracted from the single or multimodal biometric traits to indicate whether the person who is present at the time of capture is actually alive. Usually software based techniques which use extracted features to distinguish between real and fake traits are commonly employed as they require less cooperation from the user, which makes them faster and less intrusive.

Even though multi-modalities provide remarkably low False Acceptance Rate in a tampering hypothesis[6]. Reconstruction of the original template, and if a single trait is revealed, risk of exposure of combined template is greatly complicated. Additionally, cryptosystems for multi- modalities are employed for template protection as they make the system more efficient and simultaneously privacy friendly [7].

As defined in [8], biometric cryptosystems involves binding of a key to the biometric feature or generation of the key from the biometric feature. Also the art of transforming the features into new format so that even if they are stolen by attacking the database, attacker needs to decrypt the encrypted features with right key is known as crypto-bio systems. Further cryptographic systems [9] are classified into two categories symmetric key systems and asymmetric key systems which can be explained as follows:

1.1 SYMMETRIC KEY ENCRYPTION

In symmetric key cryptography, the same key is used for both encryption and decryption purposes. The techniques of symmetric cryptosystems are more robust against possible attacks, but symmetric crypto-bio systems mainly suffer from limitation of brute forcing the secret key[10]. Due to this fact, cryptographic systems suffer from critical security issue as same key known as secret key is used between two parties as in case of DES algorithm.

1.2 ASYMMETRIC KEY ENCRYPTION

In asymmetric key cryptography, different keys are used for encryption and decryption purposes as same key is not shared between two parties in this case. These methods make use of two keys: Public key and Private key. Public key is used to encrypt the features and Private Key is used to decrypt the features[11]. The asymmetric key encryption methods overcome the limitation caused by symmetric key encryption as features encrypted by public can only be decrypted by using same algorithm but matching private key. These methods suffer from the limitation that they are slow as compared to symmetric ones but provide more reliable systems.

III PROPOSED WORK

The proposed framework involves combination of liveness detection and crypto-biometric modules for the fusion of face and fingerprint modalities in order to ensure both security and privacy. The biometric data collected from both the traits is encrypted using RSA method to form the multi-modal biometric cryptosystem. This data after decryption using appropriate key is passed through liveness detection technique. And the scores produced during the employed anti-spoofing method will detect whether the provided trait is live or fake. Based on this anti-spoofing judgement, genuine traits are then matched with the stored template if appropriate key is generated otherwise given traits are

rejected. Thus, the overall architecture of proposed work is shown by Figure 3, in which two major blocks liveness detection and template protection using RSA algorithm are integrated.

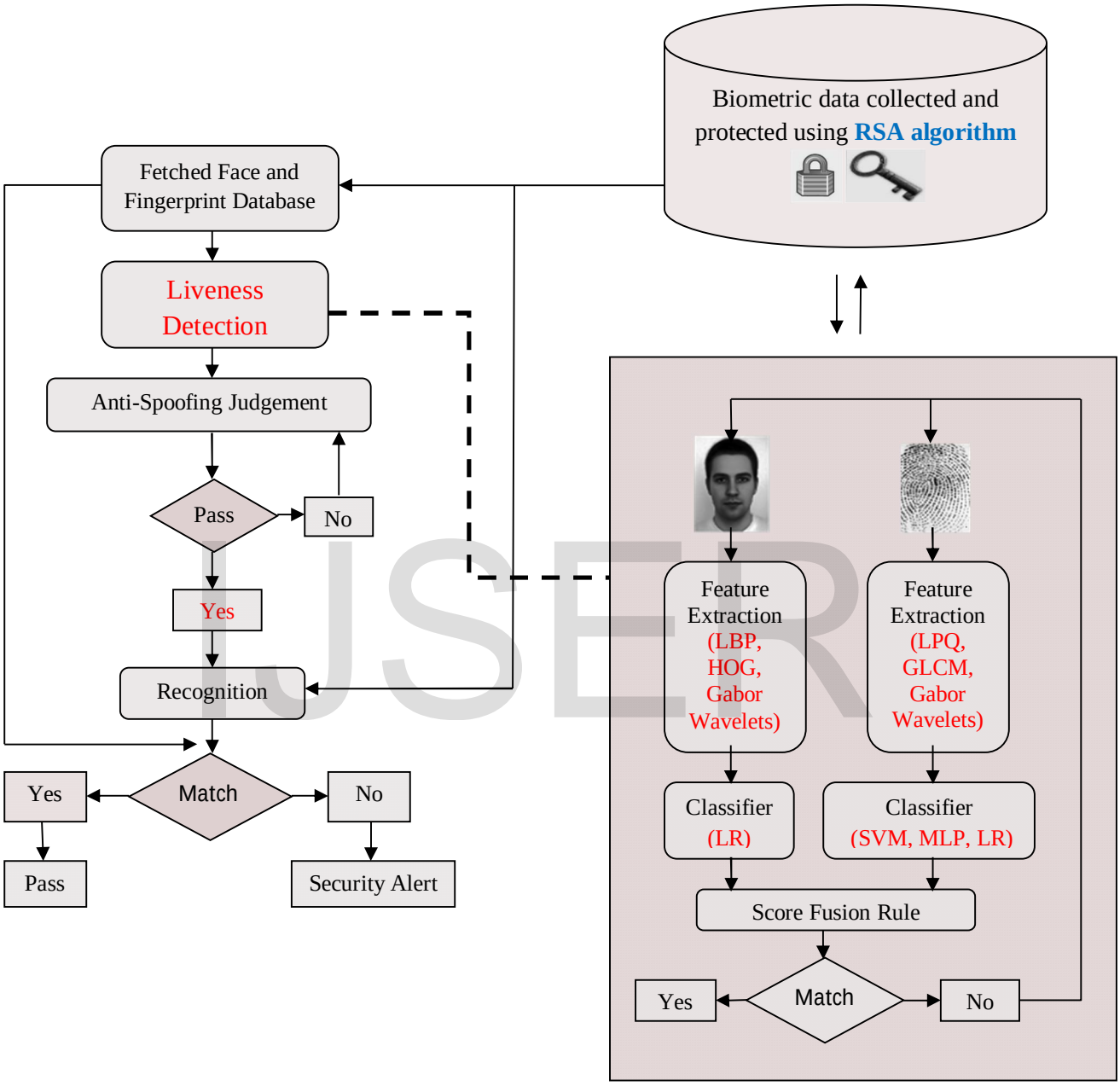

Figure 3: Overall architecture diagram of the proposed approach.

3.1 TEMPLATE PROTECTION USING RSA ALGORITHM

In this paper, we propose an efficient technique named RSA which provide best possible security using asymmetric (public) key [12]. A user in RSA creates and then declares a product of two large prime numbers with auxiliary value as a public key. The prime factors used should be kept secret. Also public key used to encrypt the message can be accessed by any party, but with currently published methods, larger length of the key makes the system more feasible.

3.1.1 OPERATION

RSA algorithm operates in three phases: first phase involves key generation, second phase involves encryption and third phase involves decryption.

3.1.2 KEY GENERATION

RSA makes use of public key and private key. Public key used is known to everyone as its is used for encrypting features whereas decryption of these features certain amount of time using private key. The overall key generation method can be explained as follows:

STEP 1: Select two different prime numbers p and q. For security purposes, these two integers should be large and randomly chosen. Primality test can be used to efficiently detect prime numbers.

STEP 2: Calculate $n = p \times q$

n is the modulus of public key and private key used for encryption and decryption and its length is expressed in bits.

STEP 3: Compute the totient function $\phi(n) = \phi(p)\phi(q) = (p-1)(q-1)$ and its value is kept private.

STEP 4: Select an integer e which is co-prime to $\phi(n)$, such that $1 < e < \phi(n)$ and $\gcd(e, \phi(n)) = 1$ (where gcd is greatest common denominator).

- e is released as the public key exponent.

STEP 5: Calculate d, $1 < d < \phi(n)$ such that $d \times e = 1 \bmod(\phi(n))$.

- d is kept as private key exponent.

The public key is (n, e) and the private key is (n, d) the values of p, q and $\phi(n)$ are private.

3.1.3 ENCRYPTION

Encryption of plaint text m such that m<n can be given by:

$$c = m^e \bmod(n)$$

3.1.4 DECRYPTION

Decryption of cipher text c to obtain the plain text m is given by:

$$m = c^d \bmod(n)$$

3.2 LIVENESS DETECTION

In this paper, software based liveness detection technique is involved in which features extracted from standard datasets consisting live and fake traits is used to distinguish between genuine and imposter user's. The overall detection involves classification of traits during training and then fusion of provided scores generated during testing; user is classified as genuine if the match score is greater than some threshold value otherwise stated as imposter.

3.2.1 FEATURE EXTRACTION

- Fingerprint feature extraction- The proposed method extracts global properties and local texture details using three methods selected as excellent methods (LPQ [13], Gabor wavelet based [14], GLCM [15]) to make maximal use of the fusion technique.

- Face feature extraction- The proposed method adopts two powerful texture features, LBP's [16] and Gabor wavelets [17] for describing micro-textures as well as macroscopic information. In addition, local shape description is provided using HOG [18].

3.2.2 FEATURE CLASSIFICATION

In the proposed work, three robust classifiers are used 1) SVM 2) LR and 3) Multi-layer Perceptron.

A Support Vector Machine (SVM) is a distinctive classifier conventionally defined by a segregating hyperplane. In other words, samples are trained (using supervised learning), in such a way that it produces an optimal hyperplane which categorizes new samples. An SVM as a classifier is a representation of the samples as a point in space in such a way that the distinct categories are divided by a clear gap.

Multi-layer perceptron is also based on supervised learning using feed-forward artificial neural network. MLPC uses backpropagation for training of data. It consists of multiple layers of nodes. Each layer if fully connected to the next one. Further, it can train a non-linear function approximator for classification purposes. Also algorithm supports multi-label classification in which a sample can be classified among more than one class.

Logistic regression classification model is used to estimate the probability of a binary response based on one or more independent features. Logistic regression measures the relationship between the categorical dependent variable and one or more independent variables by estimating probabilities using a logistic function, which is the cumulative logistic distribution.

3.2.3 SCORE FUSION

In the proposed work, two different score level fusion rules are used to fuse scores coming from the classifiers. Following Kittler et al.'s classical framework [19], sum and median rules are given by:

$$F_{sum}(\vec{s}) = \frac{1}{n}\sum_{i=1}^{n} s_i \; ; \tag{1}$$

$$F_{median}(\vec{s}) = \underset{i=1}{\overset{n}{med}}\, s_i . \tag{2}$$

For an integration of counter-spoofing techniques into biometric fusion, the paper involves a variation of the median rule, called median filter for higher spoofing-resistance:

$$F_{mf}(\vec{s}) = \frac{1}{\sum_{i=1}^{n} M(\vec{s}, s_i)} \sum_{i=1}^{n} M(\vec{s}, s_i) s_i . \tag{3}$$

$$M(\vec{s}, s_i) = \begin{cases} 1, \; if \left| s_i - \underset{j=1}{\overset{n}{med}} s_j \right| < \phi, \\ 0, \; else. \end{cases} \tag{4}$$

3.2.4 ANTI-SPOOFING JUDGEMENT

The function of the fusion module F is to generate a decision score based on the vectors of matching scores $\vec{s} = (s_1, s_2, s_3, ...s_n)$ used for verification V based on a threshold η :

$$S = \begin{cases} genuine, \quad if \; s \geq \eta; \\ impostor, \; else. \end{cases} \tag{5}$$

where S is the final decision of liveness detection module[20].

IV EXPERIMENTAL RESULTS

In order to test the stability of proposed approach under spoofing attacks, a cryptographic method using RSA algorithm along with a custom liveness detector is employed. The multimodal database used for the proposed framework is CASIA Face Anti-Spoofing Database for face and Fingerprint Liveness Detection Competition 2015 for fingerprint. The database consists of 35 real and 5 spoofed samples of both the traits. The evaluation of the proposed multimodal biometric system is carried out using Receiver Operating Characteristics (ROC) by varying the system threshold η introducing the relationship between Genuine Acceptance Rate (GAR, the percentage of genuine users being accepted) and False Acceptance Rate (FAR, percentage of impostors being accepted). In the proposed system m is the number of spoofed samples out of n total number of samples. In a similar manner (S)EER is referred to as the (Spoof) Equal Error Rate where GAR=FAR, provided lower the value of EER higher the accuracy of biometric system.

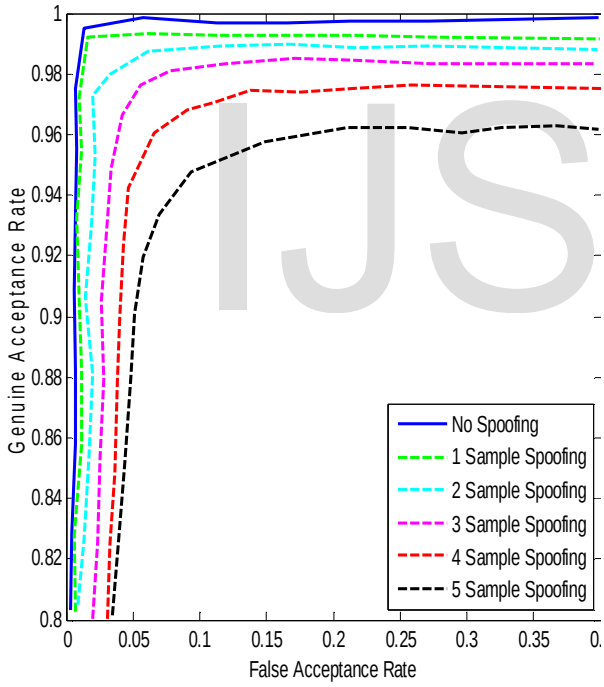

FIGURE 4: ROC for partial multi-biometric after liveness detection.

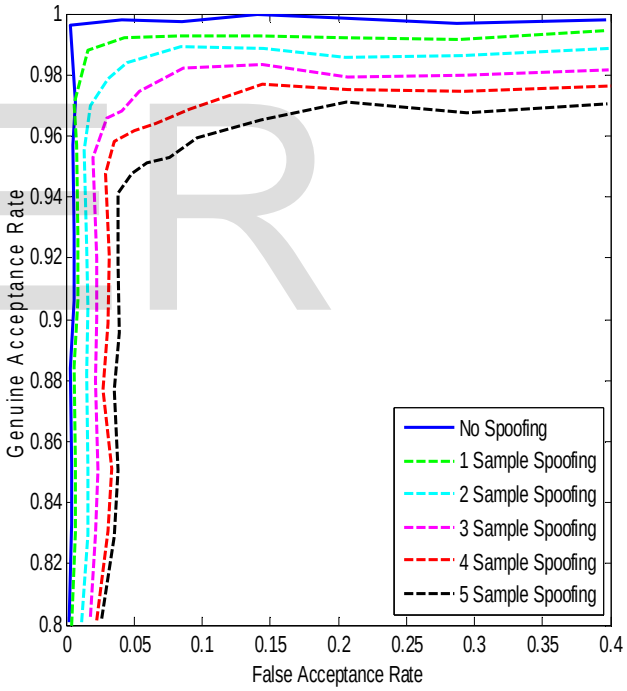

FIGURE 5: ROC for partial multi-biometric after integration of liveness detection and cryptography(RSA).

From the ROC curves shown in figure 4 and figure 5 it can be clearly stated that that the proposed approach is capable to ensure the security and privacy in terms of genuine acceptance rate which is almost 100% in no spoofing scenario and decreases less deliberately with the increase in number of added spoofed samples in comparison to multi-modal system employing liveness detection only. Various plots for EER values of the proposed system with respect to system threshold values at five different spoofing instances are significantly shown in figure 6.

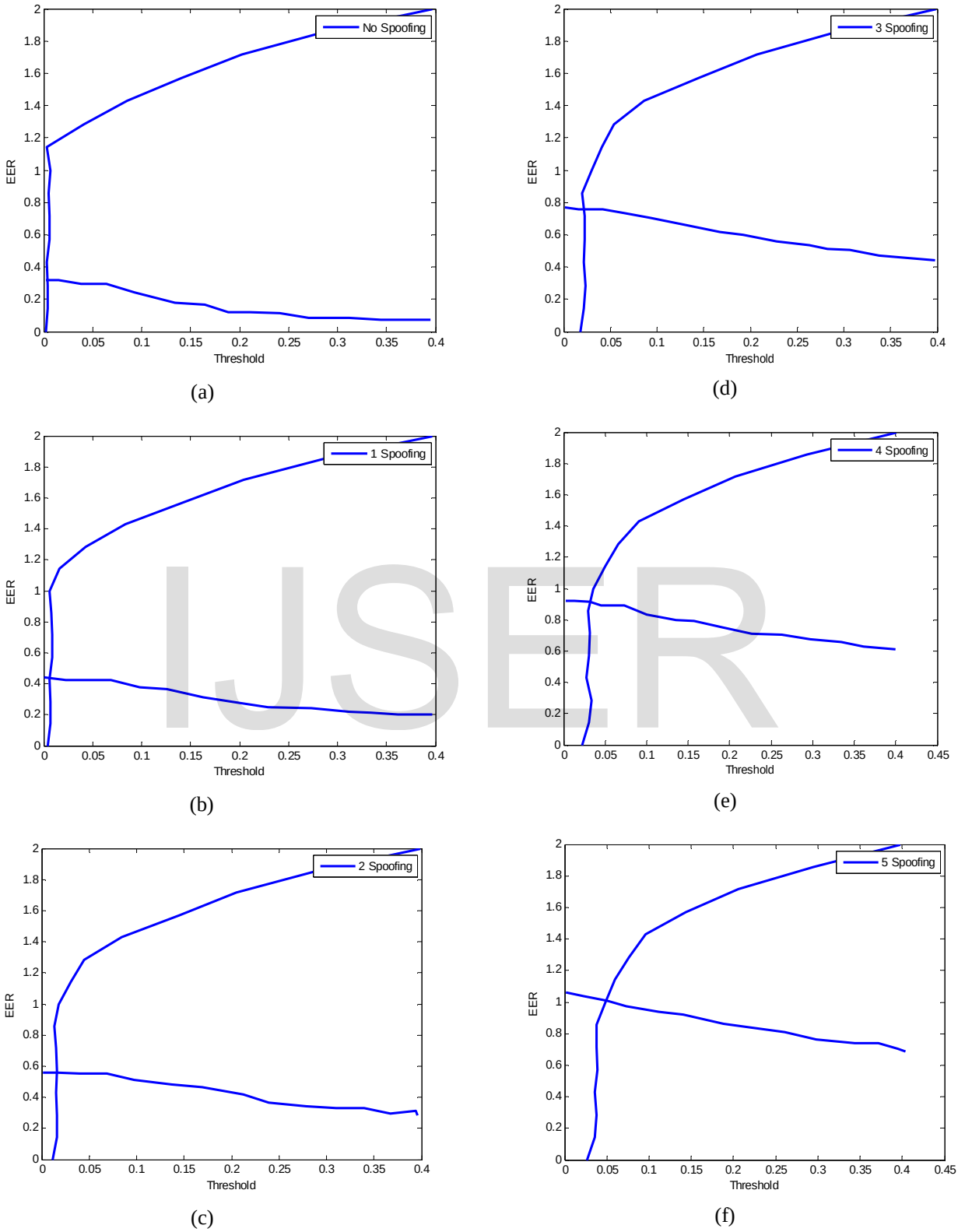

FIGURE 6: EER curves of proposed system (face-and-finger fusion) on the test set varying the number m of spoofed samples where (m=0,1,2,3,4,5) for (a),(b),(c),(d),(e) and (f).

Comparison of Proposed system performance with traditional methods in terms of EER:

In contrast to previous experiments on fusion of face and fingerprints, median filtering rule has shown to be even more successful in combining scores even though it comes at the cost of evidently degraded initial performance. The proposed method clearly outperforms existing sum and median filtering rules of liveness detection in worst case scenario (i.e., both the traits to be combined are spoofed) by providing minimum value of EER (1%) thereby maintaining better tolerance vs. spoofing attempts.

Number of Spoofed samples	Liveness Detection using sum rule (EER)[20]	Liveness Detection using median filtering (EER)[20]	Proposed Liveness Detection + RSA template protection (EER)
m=0	0	0.47	0.31
m=1	2.41	0.83	0.43
m=2	5.03	1.07	0.55
m=3	7.62	1.31	0.75
m=4	10.32	1.67	0.91
m=5	12.49	1.69	1

V CONCLUSION

Experiments in this paper show that template protection along with liveness detection provides excellent results to ensure security and privacy aspects to the system exposed to malicious adversaries. Even if m out of n samples of both face are fingerprint traits are spoofed, proposed system can't be easily circumvented by the attacker as it provides an EER between 0.31-1% which is correspondingly inferior than traditional methods of anti-spoofing. Further, incorporation of asymmetric key method of encryption (RSA) involves generation of appropriate key if user is accepted as genuine during authentication which resist the risk of exposure of combined template even if a single trait is revealed to make the system more robust to spoofing due to leakage of information.

REFERENCES

[1] A. K. Jain, P. Flynn and A. A. Ross, *Handbook of biometrics. Secaucus,* NJ, USA: Springer-Verlag New York, Inc, 2007.

[2] P. Campisi, Ed., *Security and Privacy in Biometrics*. New York: Springer, 2013.

[3] S. G. Kanade, D. Petrovska-Delacrétaz and B. Dorizzi, "Enhancing information security and privacy by combining biometrics with cryptography," *Synthesis Lectures on Information Security, Privacy, and Trust,* vol. 3, pp. 1-140, 2012.

[4] Z. Akhtar, G. Fumera, G. L. Marcialis, and F. Roli, "Evaluation of serial and parallel multibiometric systems under spoofing attacks" In IEEE Fifth International Conference on Biometrics: Theory, Applications and Systems, BTAS 2012, Arlington, USA, pp. 283-288, 2012.

[5] J. Galbally, S. Marcel and J. Fierrez, "Biometric antispoofing methods: A survey in face recognition," *IEEE Access,* vol. 2, pp. 1530-1552, 2014.

[6] A. Nagar, K. Nandakumar and A. K. Jain, "Multibiometric cryptosystems based on feature-level fusion," *IEEE transactions on information forensics and security,* vol. 7, pp. 255-268, 2012.

[7] C.-A. Toli and B. Preneel, "Provoking security: Spoofing attacks against crypto-biometric systems," in *Internet Security (WorldCIS), 2015 World Congress on*, 2015.

[8] A. Cavoukian, A. Stoianov, in ed. by S. Li, A. Jain, *Encyclopedia of Biometrics* (Springer,New York), pp. 260–269, 2009.

[9] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE transactions on Information Theory,* vol. 22, pp. 644-654, 1976.

[10] Richard Jiang,Somaya Al-maadeed,Ahmed Bouridane, Danny Crookes, Azeddine Beghdadi, "biometric security and privacy", Springer International Publishing Switzerland 2017.

[11] Nasir, M. S., & Kuppuswamy. P, "Implementation of Biometric Security using Hybrid Combination of RSA and Simple Symmetric Key Algorithm" *International Journal of Innovative Research in Computer and Communication Engineering, 1*(8), pp.1741-1748,2013.

[12] X. Zhou and X. Tang, "Research and implementation of RSA algorithm for encryption and decryption," in *Strategic Technology (IFOST), 2011 6th International Forum on*, 2011.

[13] L. Ghiani, G. L. Marcialis and F. Roli, "Experimental results on the feature-level fusion of multiple fingerprint liveness detection algorithms," in *Proceedings of the on Multimedia and security*, 2012.

[14] J.Daugman, "Complete discrete 2-d Gabor transforms by neural networks for image analysis and compression",IEEE Trans.Acoust.Speech Signal Process ,vol. no. 7, pp. 1169–1179,1988.

[15] Nikam, Shankar Bhausabheb, and Suneeta Agarwal. "Wavelet energy signature and GLCM features-based fingerprint anti-spoofing." *Wavelet Analysis and Pattern Recognition, ICWAPR'08. International Conference on*. IEEE, vol. 2,2008.

[16] I. Chingovska, A. Anjos and S. Marcel, "On the effectiveness of local binary patterns in face anti-spoofing," in *Biometrics Special Interest Group (BIOSIG), 2012 BIOSIG-Proceedings of the International Conference of the*, 2012.

[17] B. S. Manjunath and W.-Y. Ma, "Texture features for browsing and retrieval of image data," *IEEE Transactions on pattern analysis and machine intelligence,* vol. 18, pp. 837-842, 1996.

[18] N. Dalal and B. Triggs, "Histograms of oriented gradients for human detection," in *Computer Vision and Pattern Recognition, CVPR 2005. IEEE Computer Society Conference on*, 2005.

[19] J. Kittler, M. Hatef, R. P. W. Duin and J. Matas, "On combining classifiers," *IEEE transactions on pattern analysis and machine intelligence,* vol. 20, pp. 226-239, 1998.

[20] P. Wild, P. Radu, L. Chen and J. Ferryman, "Robust multimodal face and fingerprint fusion in the presence of spoofing attacks," *Pattern Recognition,* vol. 50, pp. 17-25, 2016.