On the Privacy Protection of Biometric Traits: Palmprint, Face, and Signature

Saroj Kumar Panigrahy, Debasish Jena,
Sathya Babu Korra, and Sanjay Kumar Jena

Department of Computer Science & Engineering
National Institute of Technology Rourkela, 769 008, Orissa, India
{skp.nitrkl,debasishjena}@hotmail.com, {ksathyababu,skjena}@nitrkl.ac.in

Abstract. Biometrics are expected to add a new level of security to applications, as a person attempting access must prove who he or she really is by presenting a biometric to the system. The recent developments in the biometrics area have lead to smaller, faster and cheaper systems, which in turn has increased the number of possible application areas for biometric identity verification. The biometric data, being derived from human bodies (and especially when used to identify or verify those bodies) is considered personally identifiable information (PII). The collection, use and disclosure of biometric data — image or template, invokes rights on the part of an individual and obligations on the part of an organization. As biometric uses and databases grow, so do concerns that the personal data collected will not be used in reasonable and accountable ways. Privacy concerns arise when biometric data are used for secondary purposes, invoking function creep, data matching, aggregation, surveillance and profiling. Biometric data transmitted across networks and stored in various databases by others can also be stolen, copied, or otherwise misused in ways that can materially affect the individual involved. As Biometric systems are vulnerable to replay, database and brute-force attacks, such potential attacks must be analysed before they are massively deployed in security systems. Along with security, also the privacy of the users is an important factor as the constructions of lines in palmprints contain personal characteristics, from face images a person can be recognised, and fake signatures can be practised by carefully watching the signature images available in the database. We propose a cryptographic approach to encrypt the images of palmprints, faces, and signatures by an advanced Hill cipher technique for hiding the information in the images. It also provides security to these images from being attacked by above mentioned attacks. So, during the feature extraction, the encrypted images are first decrypted, then the features are extracted, and used for identification or verification.

Keywords: Biometrics, Face, Palmprint, Signature, Privacy Protection, Cryptography.

S. Ranka et al. (Eds.): IC3 2009, CCIS 40, pp. 182–193, 2009.

1 Introduction

The idea of biometric identification is very old. The methods of imprints, handwritten signatures are still in use. The photographs on the identification cards are still an important way for verifying the identity of a person. But developing technology is paving the way for automated biometric identification and is now a highly interested area of research. Biometric techniques are more and more deployed in several commercial, institutional, and forensic applications to build secure and accurate user authentication procedures. The interest in biometric approaches for authentication is increasing for their advantages such as security, accuracy, reliability, usability, and friendliness. As a matter of fact, biometric traits (*e.g.*, fingerprints, palmprints, face), being physically part of the owner, are always available to the user who is therefore not afraid of losing them. However, compared to passwords, biometric traits cannot be strictly considered as "secrets" since often they can be inadvertently disclosed: fingerprints are left on a myriad of objects such as door handles or elevator buttons; pictures of faces are easily obtained without the cooperation of the subjects. Moreover, if they are captured or if their digital representations are stolen, they cannot be simply replaced or modified in any way, as it can be done with passwords or tokens [1]. These aspects have limited so far the number of applications in which biometric authentication procedures were allowed by privacy agencies in several countries. In addition to this, users often perceive the potential threat to their privacy and this reduces the user acceptance of biometric systems, especially on a large scale.

In a typical biometric authentication system, trusted users provide the authentication party with a sample of a biometric trait (e.g., a fingerprint scan). A digital representation of the fingerprint is then stored by the party and compared at each subsequent authentication with new fingerprint scans. The party is then in charge of protecting the database where digital representations of fingerprints are stored. If an intruder gained access to the database, she could prepare fake fingerprints starting from each of the digital images. To limit such a possibility, images of biometric traits are not stored explicitly, rather they can be stored in encrypted form. Only a mathematical description of them is used (the parameters of a model or relevant features). Such a mathematical characterisation is generally called *template* and the information contained in it is sufficient to complete the authentication process. Templates are obtained through *feature extraction* algorithms.

In addition to the potential illegitimate access by imposters, biometric systems raise issues including unintended functions, unintended applications and template sharing.

– **Unintended Functions:** Our biometric traits contain rich private information, which can be extracted from biometrics for non-authentication purposes. DNA containing all genetic information including sex, ethnicity, physical disorder and mental illness can be employed for discrimination. Certain patterns in palm lines also associate with mental disorders such as Down syndrome and schizophrenia.

- **Unintended Applications:** Some biometric traits can be collected without user cooperation. Face and iris are two typical examples. Governments and organizations can employ them for tracking.
- **Template Sharing:** Biometric templates in databases of authorized agents are possible to be shared by unauthorized agents.

1.1 Risks in Biometric Systems

Although biometric authentication approaches are much more secure than the traditional approaches, they are not invulnerable. Biometric systems are vulnerable to many attacks including replay, database and brute-force attacks. Comparing verification, fusion and identification, only limited works are related to palmprint security [2]. Fig. 1 shows a number of points, Points 1-8, all being vulnerable points as identified by Ratha *et al.* [3]. The potential attack points are between and on the common components of a biometric system, input sensor, feature extractor, matcher and database and are especially open to attack when biometric systems are employed on remote, unattended applications, giving attackers enough time to make complex and numerous attempts to break in.

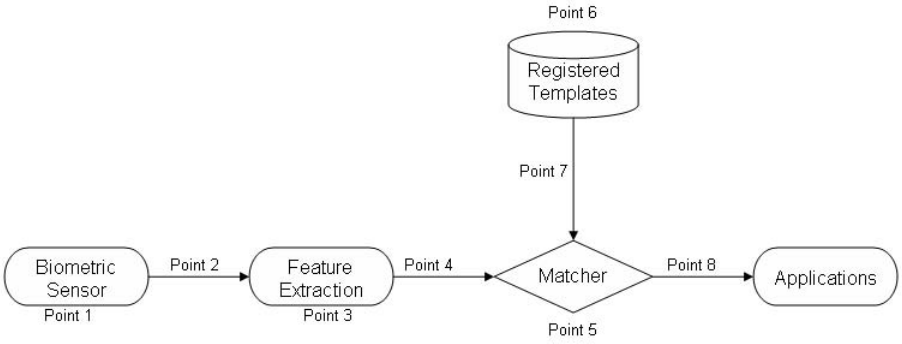

Fig. 1. Potential attack points in a biometric system

At Point 1, a system can be spoofed using fake biometrics such as artificial gummy fingerprints and face masks. At Point 2, it is possible to avoid liveness tests in the sensors by using a pre-recorded biometric signal such as a fingerprint image. This is a so-called replay attack. At Point 3, the original output features can be replaced with a predefined feature by using a Trojan horse to override the feature extraction process. At Point 4, it is possible to use both brute-force and replay attacks, submitting on the one hand numerous synthetic templates or, on the other, prerecorded templates. At Point 5, original matching scores can be replaced with preselected matching scores by using a Trojan horse. At Point 6, it is possible to insert templates from unauthorised users into the database or to modify templates in the database. At Point 7, replay attacks are once again possible. At Point 8, it is possible to override the system's decision output and to collect the matching scores to generate the images in the registered database.

Significant privacy (and operational) concerns arise with unrestricted collection and use of more and more biometric data for identification purposes. To begin with, the creation of large centralized databases, accessible over networks in real-time, presents significant operational and security concerns. If networks fail or become unavailable, the entire identification system collapses. Recognizing this, system designers often build in high redundancy in parallel systems and mirrors (as well as failure and exception management processes) to ensure availability. However, this can have the effect of increasing the security risks and vulnerabilities of the biometric data. Large centralized databases of biometric PII, hooked up to networks and made searchable in a distributed manner, represent significant targets for hackers and other malicious entities to exploit. It is also a regrettable reality that large centralized databases are also more prone to function creep (secondary uses) and insider abuse. There are also significant risks associated with transmitting biometric data over networks where they may be intercepted, copied, and actually tampered with, often without any detection. It should be evident that the loss or theft of one's biometric image opens the door to massive identity theft if the thief can use the biometric for his or her own purposes.

Both Cryptographic techniques and cancellable biometrics can be used for encryption. The difference between these two approaches is that cancellable biometrics performs matching in transform domains while cryptographic techniques require decryption before feature extraction and/or matching. In other words, decryption is not necessary for cancellable biometrics. When matching speed is an issue, e.g., identification in a large database, cancellable biometrics is more suitable for hiding the private information. And when privacy and security of palmprint database is required then cryptographic techniques can be used for encrypting the palmprint images in the database.

Various strategies have been presented to address the problem of supporting personal verification based on human biometric traits, while preserving privacy of digital templates [4]. Most approaches depend on jointly exploiting the characteristics of biometrics and cryptography [5,6]. The main idea is that of devising biometric templates and authentication procedures which do not disclose any information on the original biometric traits, for example replicating the usual approach adopted in password-based authentication system. Similarly, biometric templates are generated by using suited cryptographic primitives so as to protect their privacy and ensure that an attacker cannot retrieve any information on the original biometric trait used for the generation of the template. In this way, user's privacy is guaranteed. Moreover, even if a template is compromised (stolen, copied, etc.) it is always possible to generate a novel template by starting from the same original biometric trait.

In this paper, we propose an encryption technique to encrypt the images of palmprints , faces and signatures by a advanced version of Hill cipher algorithm for maintaining privacy, before storing in database for feature extraction. Our scheme resists the brute-force attacks and database attacks. The rest of the paper is organized as follows. Section 2 deals with description of Hill Cipher encryption

technique. In Section 3 our proposed advanced Hill cipher encryption algorithm is explained. Results are discussed in the Section 4. Section 5 gives the concluding remarks.

2 Hill Cipher

Hill ciphers are an application of linear algebra to cryptology. It was developed by the mathematician Lester Hill. The Hill cipher algorithm takes m successive plaintext letters and substitutes m ciphertext letters for them. The substitution is determined by m linear equations in which each character is assigned a numerical value ($a = 0, b = 1, ..., z = 25$). Let m be a positive integer, the idea is to take m linear combinations of the m alphabetic characters in one plaintext element and produce m alphabetic characters in one ciphertext element. Then, an $m \times m$ matrix K is used as a key of the system such that K is invertible *modulo* 26 [7]. Let k_{ij} be the elements of matrix K . For the plaintext block $P = (p_1, p_2, ..., p_m)$ (the numerical equivalents of m letters) and a key matrix K, the corresponding ciphertext block $C = (c_1, c_2, ..., c_m)$ can be computed as follows.

For Encryption: $E_K(P) = KP = C$, i.e.,

$$\begin{pmatrix} c_1 \; c_2 \; ... \; c_m \end{pmatrix} = \begin{bmatrix} k_{11} & k_{12} & ... & k_{1m} \\ k_{21} & k_{22} & ... & k_{2m} \\ ... & ... & ... & ... \\ k_{m1} & k_{m2} & ... & k_{mm} \end{bmatrix} \begin{pmatrix} p_1 \; p_2 \; ... \; p_m \end{pmatrix} \tag{1}$$

For Decryption: $D_K(C) = K^{-1}C = K^{-1}KP = P$, i.e.,

$$\begin{pmatrix} p_1 \; p_2 \; ... \; p_m \end{pmatrix} = \begin{bmatrix} k_{11} & k_{12} & ... & k_{1m} \\ k_{21} & k_{22} & ... & k_{2m} \\ ... & ... & ... & ... \\ k_{m1} & k_{m2} & ... & k_{mm} \end{bmatrix}^{-1} \begin{pmatrix} c_1 \; c_2 \; ... \; c_m \end{pmatrix} \tag{2}$$

If the block length is m, there are 26^m different m letters blocks possible, each of them can be regarded as a letter in a 26^m-letter alphabet. Hill's method amounts to a mono-alphabetic substitution on this alphabet [8].

2.1 Use of Involutory Key Matrix

Hill Cipher requires inverse of the key matrix while decryption. infact that not all the matrices have an inverse and therefore they will not be eligible as key matrices in the Hill Cipher scheme [9]. If the key matrix is not invertible, then encrypted text cannot be decrypted. In order to overcome this problem, we suggest the use of self-invertible or involutory matrix while encryption in the Hill Cipher. If the matrix used for the encryption is self-invertible, then, at the time of decryption, we need not to find inverse of the matrix. Moreover, this method eliminates the computational complexity involved in finding inverse of the matrix while decryption. A is called involutory matrix if $A^{-1} = A$. The various methods for generation of self-invertible matrix are proposed in [10].

2.2 Image Encryption Using Hill Cipher

We note that Hill cipher can be adopted to encrypt grayscale and color images. For grayscale images, the modulus will be 256 (the number of levels is considered as the number of alphabets). In the case of color images, first decompose the color image into (RGB) components. Second, encrypt each component (R-G-B) separately by the algorithm. Finally, concatenate the encrypted components together to get the encrypted colour image [11].

3 Proposed Advanced Hill Cipher Encryption Algorithm

Saeednia S. has proposed a symmetric cipher that is actually a variation of the Hill cipher. His scheme makes use of "random" permutations of columns and

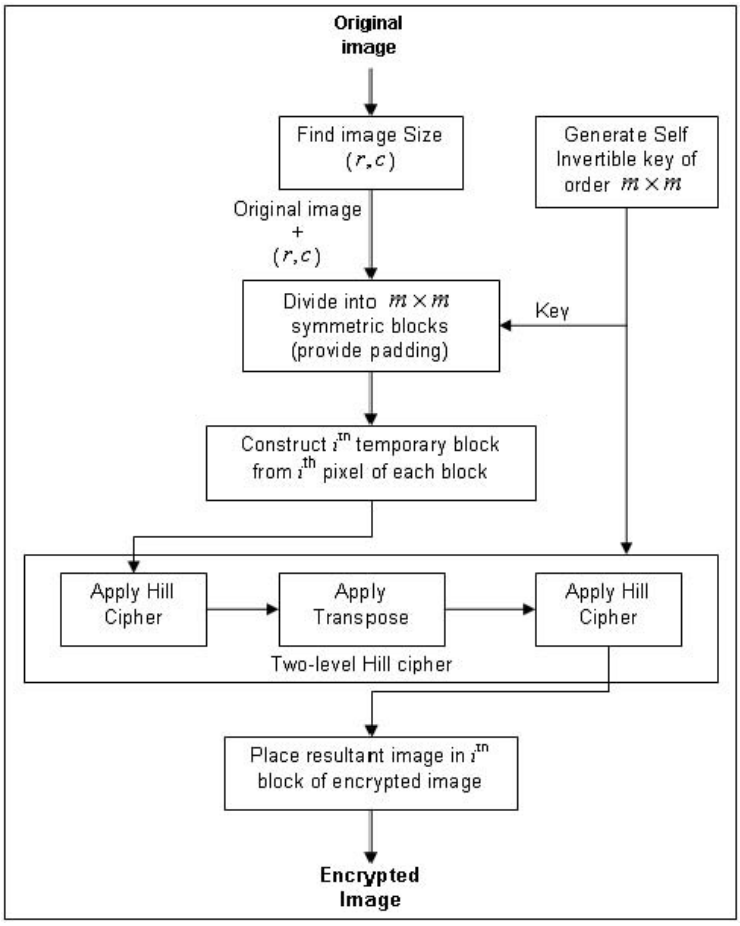

Fig. 2. Block Diagram for proposed AdvHill Cipher Encryption

rows of a matrix to form a "different" key for each data encryption. The cipher has matrix products and permutations as the only operations which may be performed "efficiently" by primitive operators, when the system parameters are carefully chosen [12].

A main drawback of Hill Cipher algorithm is that it encrypts identical plaintext blocks to identical ciphertext blocks and cannot encrypt images that contain large areas of a single colour [13]. Thus, it does not hide all features of the image which reveals patterns in the plaintext. Moreover, it can be easily broken with a known plaintext attack revealing weak security. So, Ismail et al. have proposed a variant of the Hill cipher that overcomes these disadvantages [14]. The proposed technique adjusts the encryption key to form a different key for each block encryption. It is mentioned in the paper that their proposed variant yields higher security and significantly superior encryption quality compared to the original one. But Y. Rangel-Romero *et al.* have given comments on the above proposed technique that the proposed method of encryption using modified Hill cipher still has security flaws as compared to the original Hill Cipher technique [15].

Despite Hill cipher being difficult to break with a ciphertext-only attack, it succumbs to a known plaintext attack assuming that the opponent has determined the value of p (number of alphabets) being used. We present a variant of the Hill cipher that we have named as AdvHill, which overcomes these disadvantages. Visually and computationally, experimental results demonstrate that the proposed variant yields higher security and significantly superior encryption quality compared to the original one. The algorithm and the block diagram (Fig. 2) for AdvHill are given as follows.

3.1 The AdvHill Algorithm

1. A self-invertible key matrix of dimensions m x m is constructed.
2. The plain image is divided into m x m symmetric blocks.
3. The i^{th} pixels of each block are brought together to form a temporary block.
   (a) Hill cipher technique is applied onto the temporary block.
   (b) The resultant matrix is transposed and Hill cipher is again applied to this matrix.
4. The final matrix obtained is placed in the i^{th} block of the encrypted image.
5. The steps 3 to 4 are repeated by incrementing the value of i till the whole image is encrypted.

4 Results and Discussions

We have taken different images and encrypted them using the original cipher and our AdvHill algorithm and the results are shown below in Fig. 3. It is clearly noticeable from the Fig. 3(h,i), that original Hill cipher algorithm could not be able to decrypt the images properly because of the background of the image of same colour or gray level. But our proposed AdvHill cipher algorithm could decrypt the images properly as shown in Fig. 3(m,n). Fig. 4 shows the time

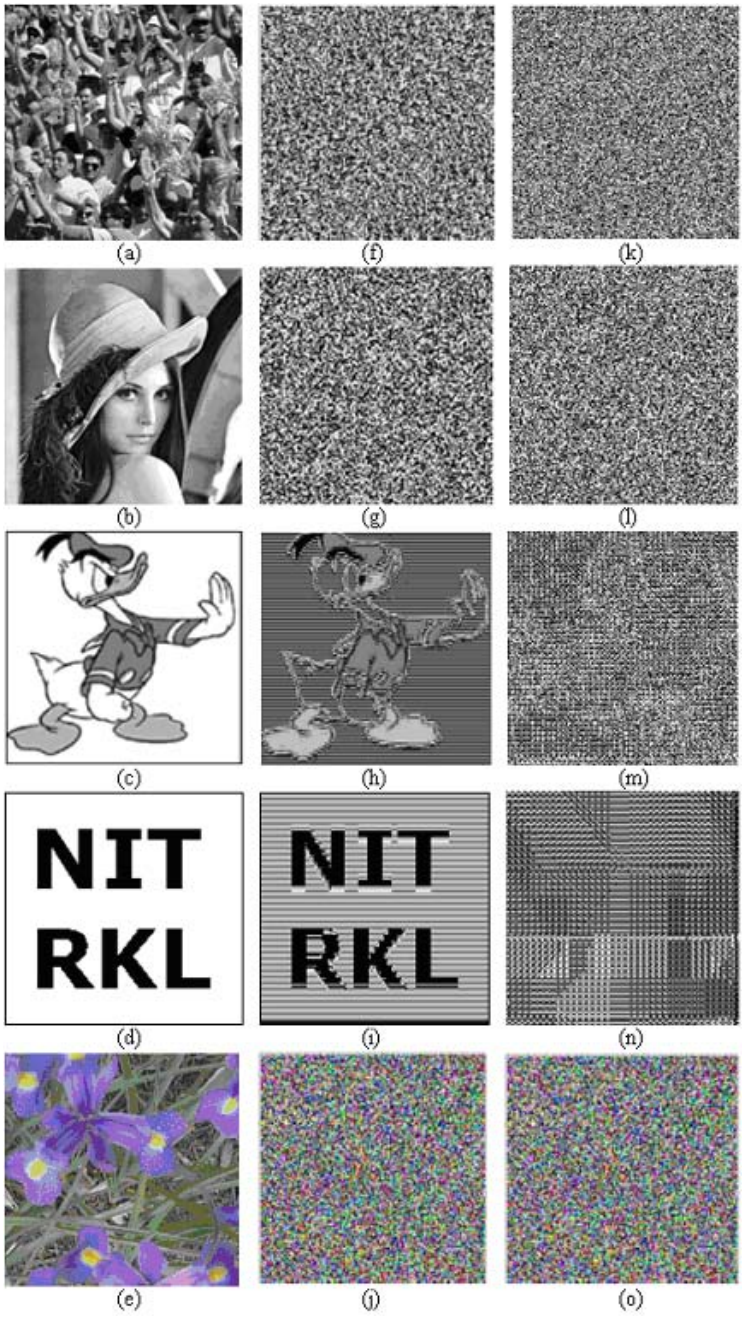

Fig. 3. Original images (a-e), corresponding encrypted images by Hill Cipher (f-j) and by AdvHill Cipher Algorithm (k-o)

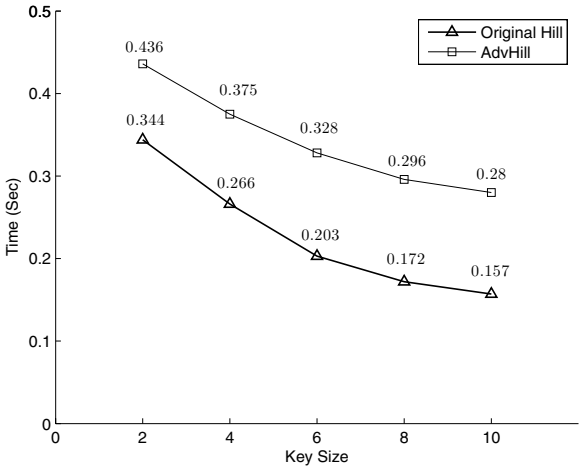

Fig. 4. Encryption time test of Lena image

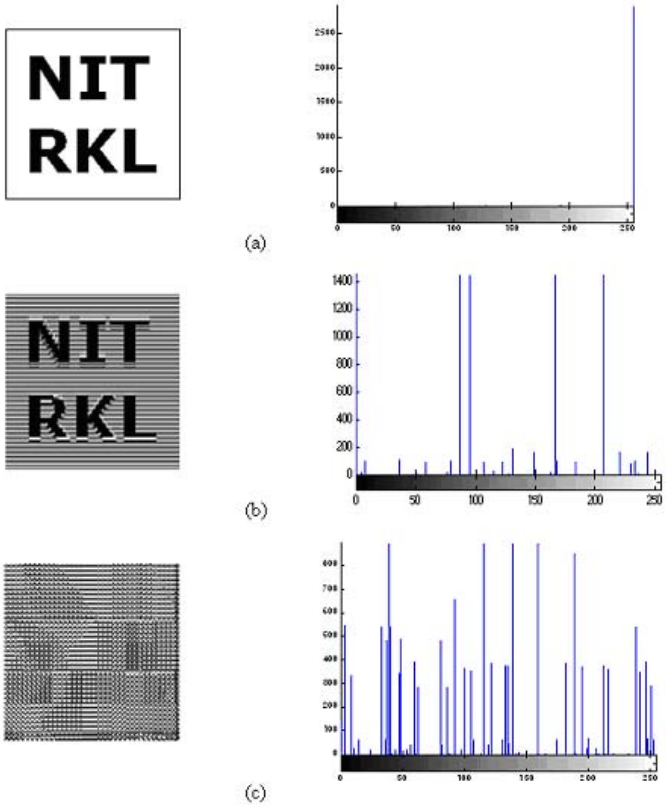

Fig. 5. Histograms of (a) original NITRKL image (b) image encrypted by original Hill cipher and (c) image encrypted by AdvHill cipher

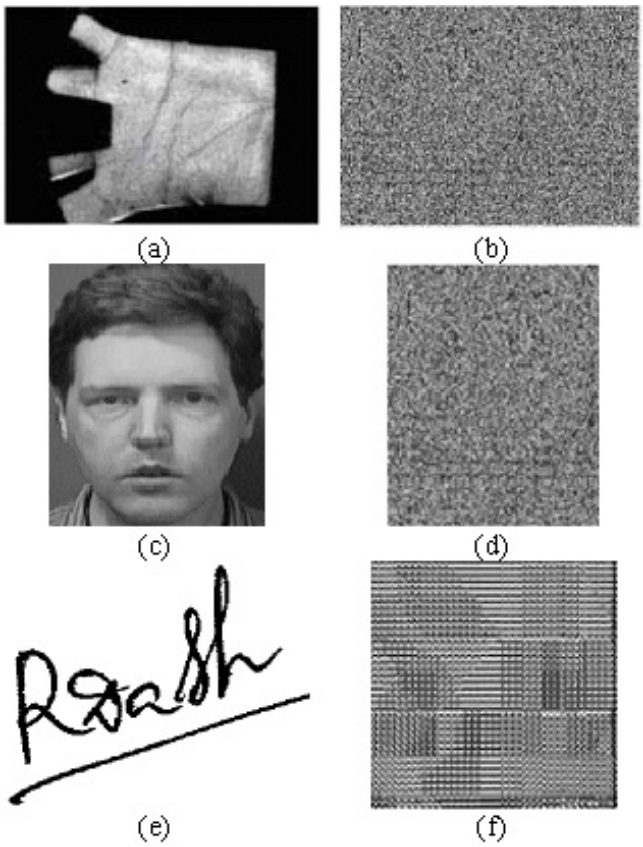

Fig. 6. Encryption of biometric images by AdvHill cipher (a) palmprint image (b) face image (c) signature

analysis for Lena image encryption by original Hill and AdvHill algorithms. It is clear that our AdvHill takes more time than that of original Hill to encrypt the image but with stronger security. Fig. 5 shows how our AdvHill algorithm is capable of decrypting the image as in the histograms it introduces more gray levels which leads to failure of frequency analysis by attackers. This shows that our image encryption scheme is stronger than the original Hill cipher and is also resistant to known-plaintext attack.

4.1 Palmprint, Face and Signature Image Encryption

From the previous section, it is clear that our AdvHill cipher algorithm works well for image encryption compared to that of original Hill Cipher algorithm. We can apply our AdvHill to any type of images for encryption. So, to provide security and maintain privacy of the biometric traits, i.e., palmprint, face and signature images of the users, we encrypt the images and then store in databases for feature

extraction as shown in Fig. 6. Before feature extraction, these encrypted images are decrypted by the same key as the key matrix is an involutory matrix. The palmprint and face images are taken from PolyU palmprint database [16] and AT&T Face database [17] respectively.

5 Conclusion

We have proposed a cryptographic which is a traditional method of encrypting images. Systems protected by cryptography store only encrypted images in databases. However, cryptography is not suitable for speed-demanding matching, e.g. real-time large-scale identification, since decryption is required before matching. Another potential solution is cancellable biometrics which can be used for encryption. Cancellable biometrics transform original templates into other domains and perform matching in the transformed domain. Although cancellable biometrics overcome the weakness of cryptography, current cancellable biometrics are still not secure enough for the palmprint identification. For example, attackers can still insert stolen templates replay and database attacks before systems can cancel the stolen templates and reissue new templates. Furthermore, current cancellable biometrics cannot detect replay and database attacks. In other words, if attackers insert unregistered templates into data links or databases, systems cannot discover the unregistered templates. To solve these problems, we can take advantages of cryptography and cancellable biometrics to design a set of security measures to prevent replay, brute force and database attacks for secure palmprint, face and signature biometric systems.

Acknowledgments. This research is supported by Department of Communication and Information Technology, Government of India, under Information Security Education and Awareness Project and being carried out at department of Computer Science and Engineering, National Institute of Technology Rourkela, Orissa, India.

References

1. Schneier, B.: The uses and abuses of biometrics. Communication of the ACM 42(8), 136 (1999)
2. Kong, A.W.K., Zhang, D., Kamel, M.: Analysis of brute-force break-ins of a palmprint authentication system. IEEE Transactions On Systems, Man and Cybernetics-Part B: Cybernetics 36(5), 1201–1205 (2006)
3. Bolle, R.M., Connell, J.H., Ratha, N.K.: Biometric perils and patches. Pattern Recognition 35, 2727–2738 (2002)
4. Uludag, U., Pankanti, S., Prabhakar, S., Jain, A.: Biometric cryptosystems: Issues and challenges. In: Proceedings of the IEEE, Special Issue on Enabling Security Technologies for Digital Rights Management, June 2004, vol. 92, pp. 948–960 (2004)
5. Juels, A., Wattenberg, M.: A fuzzy commitment scheme. In: Proceedings of the 6th ACM conference on Computer and communications security (CCS 1999), pp. 28–36. ACM Press, New York (1999)

6. Hao, F., Anderson, R., Daugman, J.: Combining cryptography with biometrics effectively. Technical Report UCAMCL-TR 640, Computer Laboratory, University of Cambridge, United Kingdom (July 2005)
7. Petersen, K.: Notes on number theory and cryptography (2002), http://www.math.unc.edu/Faculty/petersen/Coding/cr2.pdf
8. Menezes, A.J., Oorschot, P.V., Stone, S.V.: Handbook of Applied Cryptography. CRC Press, Boca Raton (1996)
9. Schneir, B.: Cryptography and Network Security, 2nd edn. John Wiley & Sons, Chichester (1996)
10. Acharya, B., Patra, S.K., Panda, G., Panigrahy, S.K.: Novel methods of generating self-invertible matrix for hill cipher algorithm. International Journal of Security 1(1), 14–21 (2007)
11. Li, S., Zheng, X.: On the security of an image encryption method. In: Proceedings of the IEEE International Conference on Image Processing (ICIP 2002), vol. 2, pp. 925–928 (2002), http://www.hooklee.com/Papers/ICIP2002.pdf
12. Saeednia, S.: How to make the hill cipher secure. Cryptologia 24(4), 353–360 (2000)
13. Panigrahy, S.K., Acharya, B., Jena, D.: Image encryption using self-invertible key matrix of hill cipher algorithm. In: Proceedings of the 1st International Conference on Advances in Computing (ICAC 2008), Chikhli, India, pp. 1–5 (2008)
14. Ismail, I.A., Amin, M., Diab, H.: How to repair the hill cipher. Journal of Zhejiang Univ. Science A 7(12), 2022–2030 (2006)
15. Rangel-Romero, Y., et al.: Comments on how to repair the hill cipher. Journal of Zhejiang University SCIENCE A, 1–4 (2007)
16. Palmprints. Hongkong PolyU Palmprint Database, http://www.comp.polyu.edu.hk/~biometric
17. Faces, Cambridge AT&T Lab Face Database, http://www.cl.cam.ac.uk/research/dtg/attarchive/facedatabase.html