International Journal of Security and Its Applications
Vol.8, No.6 (2014), pp.51-60
http://dx.doi.org/10.14257/ijsia.2014.8.6.05

Implementation of Biometric Techniques in Social Networking Sites

Shilpi Sharma[1] and J. S. Sodhi[2]

Computer Science and Engineering Department, ASET, Amity University Noida, India
AKC Data Systems, Amity University, Noida, India
ssharma22@amity.edu, jssodhi@akcgroup.com

Abstract

With the advancement of technologyprivacy threats arise while establishing communication in social networking sites. For the developers of authentication systems user's privacy and authentication have evolved as a major problem and area of concern. This research is based on an attempt to discuss the implementation of different biometric verification techniques in order to perform the authentication of users in social networking sites. It decreases the chances of illegal impersonation thus enhancing the privacy of an individual's personal data. The prime objective of this paper is to provide a new revolution in social networking sites by suggesting remedial measures for the security threats faced in the sites such as Facebook, MySpace, Twitter, Hi5, LinkedIn, Orkut, Tumbler, Flikeretc so that the goal of communication can be achieved without any security threat in mind. Application of securedbiometricsenables confirmation of personal detailsfor establishing the identity of an individual.

Keywords: *biological characteristics, authentication, encryption, privacy, Social Networking Sites, BioCrytoSystems*

1. Introduction

Over the past few years, communication through social networking sites has become increasingly popular. Due to their popularity, it's hard to Figure out the fallacies in the existing system and design a new and improved framework that can produce better results. Members use social networking sites for posts, videos, photographs and many other purposes. Existing security techniques have certain deficiencies due to which their reliability in a widely-networked social media is questionable. In the present scenario, we are facing majority of crimes related to security issues due to leakage of passwords or illegal authentications. This research paper brings the implementation of biometric technology close to social networking sites so that suitableuser authentication can be done [1] in order to save our data from malicious users and other cyber attacks. Biometrics is capable of significantlyreducing security breaches without unjustifiably affecting privacy. Biometric authentication aids the processes of identifying an individual's identity, authenticating users and non-refutation in information protection.

Biometric authentication [2, 3] refers to verifying persons based on their physiological and behavioral characteristics such as face, fingerprint, hand geometry, iris, keystroke, signature, voice, *etc.*, It is inherently more reliable than password-based authentication, as biometric characteristics cannot be lost or forgotten; they are exceptionally difficult to copy, share, and require the person being authenticated to be present at the time and point of authentication. It is difficult to forge biometrics and it is unlikely for a user to repudiate having accessed the

ISSN: 1738-9976 IJSIA

digital content using biometrics [18]. Many algorithms like Adaptive Multimodal Biometric Fusion Algorithm (AMBF), [19] random multi space quantization (RMQ) bio hashing algorithm [20], Key binding algorithm for fingerprint matching system by Soutar, *et al.*, in [21, 22] and [23] and many other algorithms were designed but are not yet implemented in Social networking Sites.

The aim of this paper is to provide useful information about security issues through biometric and bio cryptograph in the area of Social networking Sites. In this paper we have provided some recommendations for implementation and best practices to reduce the security risks to users.

2. Overview

Biometrics is a Greek word in which bios means "life" and metronmeans "measure", refers to two very differentfields of study and application. It represents biological studies *i.e.*, the collection, synthesis, analysis and management of quantitative dataon biological communities such as animals orforests. Biometrics in reference to biological sciences is somewhat simply viewed as "biological statistics" [4]

Authentication is to verify the claims that are true.Password leakage is becoming a very serious problem for the users of social networking sites. If a person can access the password of any other person, he tries to login through his account and discloseconfidential and private data, thus violating the terms and conditions of the sites which may resultssecurity threats for the fatality users.

By 2015 the password authentication will be replaced by biometric system that can identify individuals based on unique biological features, mentioned by IBM in Biometrics Upgrade.com.

The authenticity of the social networking user can be determined by using biometric technology. That needs to be implemented with social networking sites for user login rather than using text passwords,which increases privacy and security without compromising the benefits of information sharing through SNSs. Biometric provides certain schemes for identification of the authenticated and correct users. Using biometric schemes, only the correct user's entry is allowed through his account. Thus, no one can take the advantage of others account and cannot access his personal and private information.

Biometrics refers to authentication techniques that rely on measurable physical characteristics that can be automatically checked. In other words, "Biometrics is an automated method of recognizing a person based on physiological or behavioral characteristics" [24].

Several biometric identification schemes that can be implemented in any Social Networking Sites are in Figure 1:

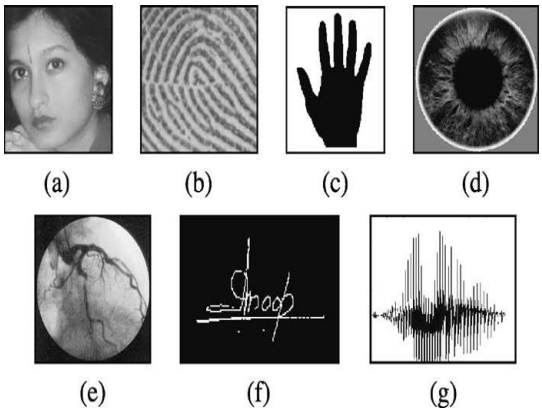

Figure 1. Examples of biometric characteristics (a) Face (b) Fingerprint (c) Hand Geometry (d) Iris (e) Retina (f) Signature (g) Voice

Face: The analysis of facial characteristics, features or patterns for the authentication of individual identity.

Fingerprint: Unique finger prints *i.e.*, by the use of ridges and valleys on the surface of fingers of every individual.

Hand Geometry: The analysis of the shape and width of the hand and the length of the fingers.

Iris: Analysis of the colored ring that surrounds the eye *i.e.*, Visual Biometric

Retina: Analysis of capillary vessels located at the back of the eye *i.e.*, Visual biometric.

Signature: The authentication of an individual by the analysis of handwriting style, avisual comparison is done between the scanned signatures.

Voice: Analysis of tone, pitch and frequency of person. The two applications of voice recognition is voice verification and voice identification

By combining biometric information with cryptographic system like shuffling scheme to transform the biometric information, where the shuffle is different for each user and application [5]. Such systems are quite successful when applied to facial recognition. However, since biometric samples are naturally variable, error correction codes had to be applied at authentication time. The conclusion was that information protection methods can be combined with key management protocols to build effective user verification with privacy protection.

3. Existing Techniques and Technologies

Security of our socially available personal content through our social media profiles can be hugely increased by implementing biometric based security techniques. Some of them are discussed in this section [2, 6]:

1. Biometric techniques can provide correct, access to personal data; fingerprints, retinal and iris scan produce absolutely unique dataset when used skillfully.
2. Minimum amount of training is required for datasets used for verification of individuals.
3. The loss of documents or physiological traits of an individual is hard to be lost or stolen.
4. Replace complex passwords which may be shared or observed.

Though these techniques have many advantages, they have certain limitations too. Some of those limitations are listed as under:

1. They provide expensive security solution.
2. For people suffering from diabetes, the eyes get affected resulting in differences.

3. The voice of a person differs with age. Also, the voice may change when the person suffers from throat infection, or if there is too much noise in the environment. In such cases, this method may not authenticate correctly.
4. The fingerprints of those people working in chemical industries are often affected. Therefore, those companies cannot use the fingerprint mode of authentication.

4. Methodology

Facebook being the hub for millions of users for networking as social media site was used for critically analyzing the security concerns related to user authentication [2].

In order to analyze the gaps in existing techniques we designed and conducted an online survey. Certain questions were created to capture the usersperception of trust, privacy concerns and sharing ofinformation. The survey indicated that users have expressed very strong concerns about privacy and safety of their personal information, but are less vigilant about safeguarding it.

Based on the survey we prepared the chart showing that 1205 respondents find the biometric techniques easy to learn and they want to see it implemented on these sites. They seem to be satisfied with the working capabilities of the technology as it not only facilitates the proper use of social networking sites but also provides them with more secure and reliable communicating platform as compared to earlier.

Q 1. Which SNSs do you use?

Figure 2. Column Chart presents the commonly used SNSs. The data depicts that out of 1205 respondents 573 are using Facebook, 271 respondents are using Twitter, 227 respondents are using LinkedIn, 62 respondents are using MySpace, 23 and 31 respondents are using Orkut and Flickr respectively 18 respondents use other SNSs.

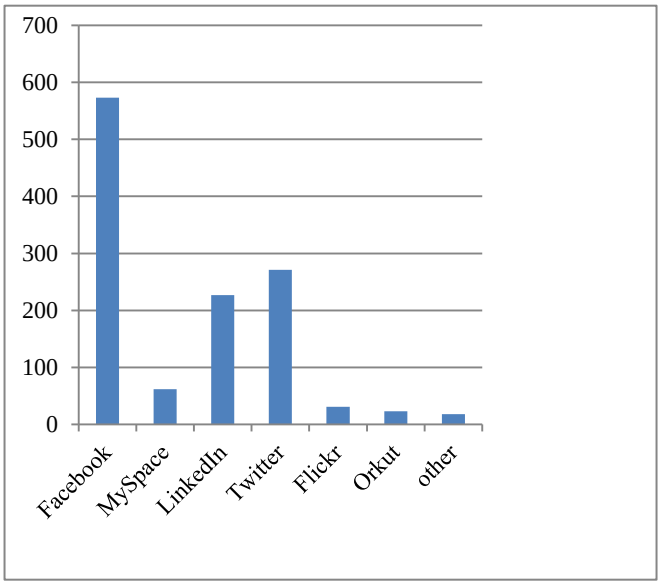

Figure 2. Column Chart Showing Most Commonly used SNS

Q2. How Many Connections (“Friends”) you have for Your Social Network profile?

Figure 3 pie chart shows that 655 respondents states that they have more than 200 friends, 252 respondents have more than 500 friends, 146 respondents have more than 100 friends , 88 and 64 respondents have friends ranging from 10 to 99 as the number of friends connections in their Social Networking Sites.

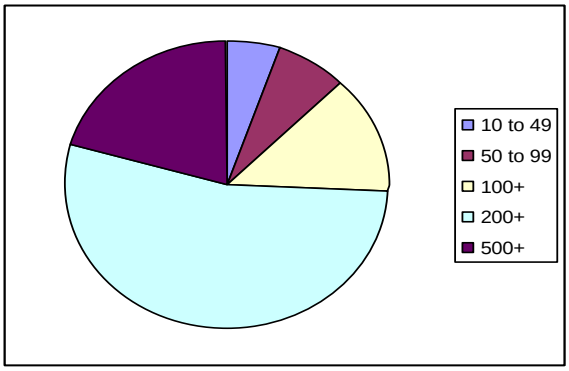

Figure 3. Pi-Chart Showing No. of Friends

Q 3. Which of the Following Types of Information and Data are Considered Personal by You?

Figure 4 Column Chart presents that 812 respondents feels that financial information are very personal, 687 feels the national identity, 638 reveals that fingerprints or other biometric information are personal whereas other agrees to mobile number, home address are their personal information that must not post in any social networking sites.

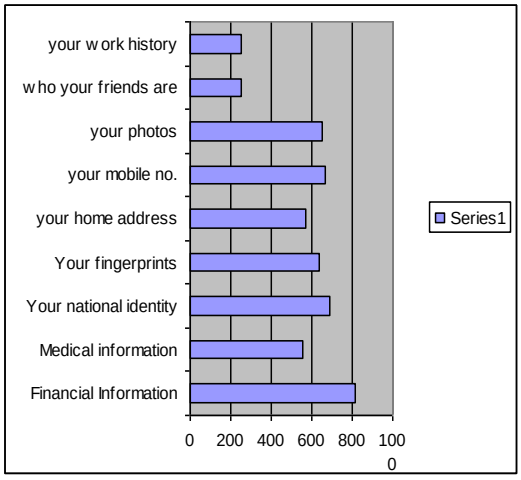

Figure 4. Bar Chart Showing Personal Ranking

Q4. How Secure do you Believe your Data on Social Networking Site is?

Figure 5 reveals that 769 respondents believe that the data stored and posted in any Social Networking Site are somewhat secure, 213 respondents filled the information is not at all secure, 136 says it's very secure whereas 87 respondents have no idea regarding the same.

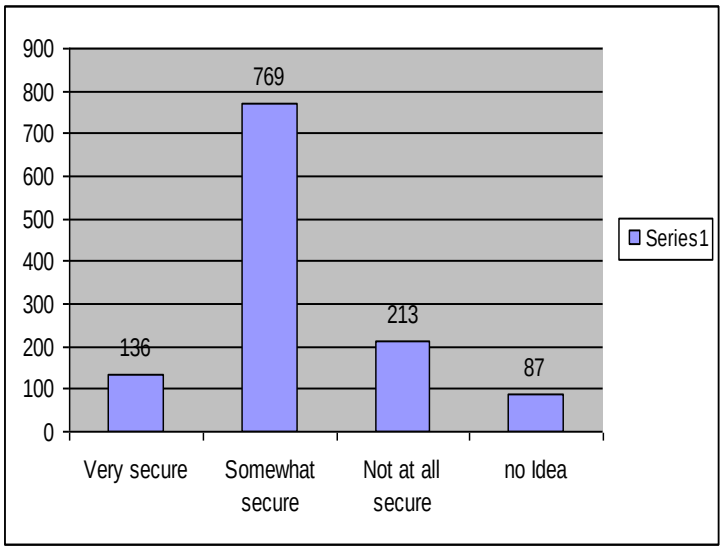

Figure 5. Column Chart Showing How Secure to Publish Data in SNS

Q5. Are You in Favor to Protect your Data using Biometric Technique?

Figure 6 presents a column chart showing user responses towards implementation of biometric technique in SNS where 754 respondents are comfortable with and 322 respondents are not aware of biometric technique whereas 139 and 79 are either not able to decide or are not satisfied with the issue.

Figure 6. User Response to Biometric

5. Applications

Biometric authentication is highly trustworthy. A secure and reliable biometric based-recognizing and matching system has immense scope in future and undisputed applications in various fields. Some of the areas of key importance, where the process of biometric verification is being employed, are areas of forensic sciences and research such as

determination of parenthood, investigation of criminal cases [17]. In Government and Commercial applications biometric recognition process plays a key role to pervade nearly all aspects of the economy and our daily lives [7].

The UDID, Unique Identification Authority of India issued Aadhar card to Indian residents that can be used for authenticate of information about the user as a biometric tool in social networking sites. It fetches the users fingerprints as well as the retinal information that can be crypto graphed along with the 12 digit number. Each user has been given a hash key value to authenticate. Encryption technologies can assist with ensuring the confidentiality of user information and also serve as a strong measure of protection against today's commonly anticipated threats, such as unauthorized access, manipulating profile data and disclosure of personal information.

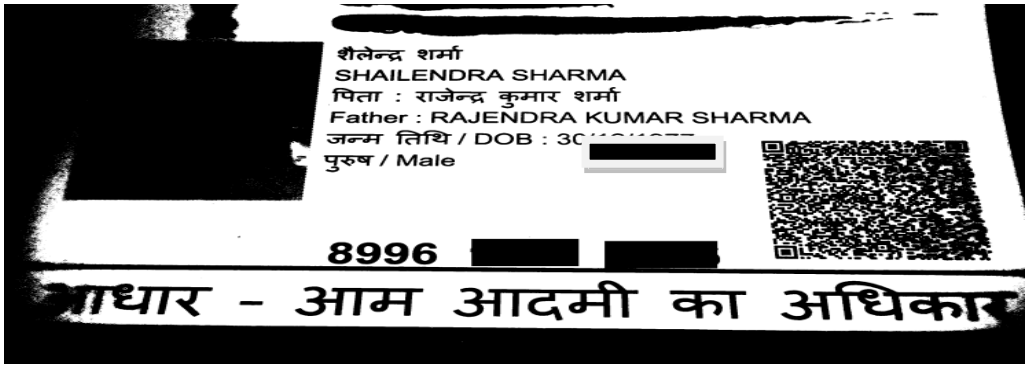

Figure 6. Aadhar Card with 12 Digit Number and Decoded Biometric Impression

6. Evaluation

The various factors described below are considered for evaluating the performance of different biometric techniques [8-10].

6.1. False Accept Rate (FAR) and False Match Rate (MAR): These constants are a measure of probability values that thesystem incorrectly declares a successful match between the selected input pattern and a non matchingpattern in the authentication system's database. It measures the percent of invalid matches. Thesesystems are dangerous since they are commonly used to forbid certain actions by disallowing people.

6.2. False Reject Rate (FRR) or False Non-Match Rate (FNMR): The probability thatthe system incorrectly declares failure of match between the input pattern and the matchingtemplate in the database. It measures the percent of valid inputs being rejected.

6.3. Relative Operating Characteristic (ROC): In general, the matching algorithmperforms a decision using some parameters (*e.g.*, a threshold). In biometric systems the FARand FRR can typically be traded off against each other by changing those parameters. TheROC plot is obtained by graphing the values of FAR and FRR, changing the variablesInternational Journal of u- and e- Service, Science and Technologyimplicitly. A common variation is the Detection Error Tradeoff (DET), which is obtainedusing normal deviate scales on both axes. This more linear graph illuminates the differencesfor higher performances (rarer errors).

6.4. Equal Error Rate (EER): The rates at which both accept and reject errors are equal.ROC or DET plotting is used because how FAR and FRR can be changed, is shown clearly.When quick comparison of two systems is required, the ERR is commonly used. It is

obtainedfrom the ROC plot by taking the point where FAR and FRR have the same value. The lowerthe EER, the more accurate the system is considered to be.

6.5. Failure to Enroll Rate (FTE or FER): The percentage of data input is consideredinvalid and fails to input into the system. Failure to enroll happens when the data obtained bythe sensor are considered invalid or of poor quality.

6.6. Failure to Capture Rate (FTC): Within automatic systems, the probability that thesystem fails to detect a biometric characteristic when presented correctly is generally treated as FTC.

6.7. Template Capacity: It is defined as the maximum number of sets of data which can beinput in to the system.

Chosen a sample group for implementation and ensure that the technology works properly for a test plan for implementing encryption solutions.

7. Future Work

Although people are feeling more comfortable using biometric security, there are still public concerns over its validity. Biometrics identity theft is much more challenging than forging a signature and illegally obtaining or copying archived biometrical prints. Thus, in future, ways are needed to combat fraud and illegal impersonation.One of the limitations of some private biometric methods is that, during the processing, the original biometric information may have to be recovered in order to perform matching, compromising the privacy protections.

Few methods allow biometric matching to be done while the data is encrypted *i.e.,* if $\boldsymbol{a}$ is a set of fingerprint features (minutiae) that describe a fingerprint offered at authentication time and $\boldsymbol{b}$ is a set of features for a fingerprint stored in a database, the difference between the two feature sets can be calculated on the encrypted sets, without ever revealing the original information [11].

8. Conclusion

In conventional and long used cryptosystems, user authentication or verifying an individual was done using secret keys possessed by the encoder, where the security of user collapses in case the keys goes missing or not kept safely or shared with different users with malicious intentions [17]. Further, the keys generated at the time of encryption of image can be stolen, or lost at a later stage. Hence, these keys fail to give the user non-refutation. The currently enforced authentication systems are mainly based on the behavior and psychology of the users (which are also known as biometric characteristics), and they give a natural solution to a majority of these problems and are capable of replacing the authentication component of the older systems. The capability of biometrics-based user authentication or personal identification techniques has helped in securing the personal and sensitive information that an individual intends to keep private. Research indicates insufficient understanding ofthe interaction of trust and privacy concern in social networking sites makes it difficult to develop an exact model of behavior and activity. The results of the study encourage the use of biometric techniques with social networking sites for proper user authentication. We also found certain limitations to the technology which requires efforts to understand and find the ways to combat fraud and biometric identity theft. We require finding the ways to come out of these limitations because though these techniques have certain disadvantages but their implementation in social networking sites during user login apart from long and hard to remember passwords will surely give a new direction to secure

networking sites and will reduce the security and privacy overhead.However, every algorithm has its own advantages and limitations. This paper signifies the necessity of BioCryptosystems in ensuring the authentication and privacy to the user. The BioCryptosystems engages the advantages of biometrics and cryptographic framework that cannot be degraded by any attacker.

The BioCryptosystems can be used to ensure user authentication and network security, though the comprised password does not affect the security level of the fuzzy vault system, since it acts as an additional layer of security. Multitude of issues occurs in combining the biometrics with the cryptographic system due to imperfect nature of biometric matching algorithms and degraded nature of biometric features. But even then biometrics is the only essential component of identity-based security system, as no other technology can be implemented in ―Identifying the authorized person based on their intrinsic distinctive traits. Therefore, it is of greater necessity for crypto biometric system to provide user authentication

Hence an interesting approach can be given by combining Biometrics, cryptography and data hiding that ensure protection against today's commonly anticipated threats. This combination may provide an effective and often complementary solution to secure the information.

References

[1] D. V. Klein, "Foiling the cracker: a survey of, and improvements to, password security," in Proc. 2nd USENIX, Workshop Security, **(1990),** pp. 5–14.
[2] A. K. Jain, R. Bolle and S. Pankanti, Eds., "Biometrics: Personal Identification in Networked Society", The International Series in Engineering and Computer Science, vol. 479, **(2005).**
[3] D. Maltoni, D. Maio, A. K. Jain and S. Prabhakar, "Handbook of Fingerprint Recognition", New York Springer-Verlag, **(2003),** pp. 1388, 1997.
[4] "Smart Cart Alliance Identity Council", Identity and Smart Card Technology and Application Glossary, **(2007),** http://www.smartcardalliance.org.
[5] **(2007),** http://biometrics.it sudparis.eu/english/index.php?menu=home.
[6] S. Sharma, A. Tripathi and L. Anusha, "Prevention of Privacy threats in Social Networking Sites", in ICACCN', 291-296/a171.pdf, **(2011)**.
[7] A. K. Jain, A. Ross and S. Prabhakar, "An introduction to biometric recognition," IEEE Trans. Circuits Syst. Video Technology, Special Issue Image- and Video-Based Biomet, vol. 14, Issue 1, **(2004)**, pp. 4–20.
[8] A. K. Jain, S. Pankanti, S. Prabhakar, L. Hong, A. Ross and J. L. Wayman, "Biometrics: a grand challenge", In Proc. of International Conference on Pattern Recognition, Cambridge, U.K. **(2004)**, pp. 935-942.
[9] J. Phillips, A. Martin, C. Wilson and M. Przybocki, "An introduction to evaluating biometric systems", IEEE Computer Society, vol. 33, no. 2, **(2000)**, pp. 56–63.
[10] J. L. Wayman, A. K. Jain, D. Maltoni and D. Maio, Eds., "Biometric Systems: Technology, Design and Performance Evaluation", New York: Springer Verlag, **(2005)**.
[11] http://blogs.teamb.com/craigstuntz/2010/03/18/38566/.
[12] http://ge.geglobalresearch.com/blog/developing-intelligent-video-algorithms-for-surveillance-applications/.
[13] I. Pentina, O. Basmanova and L. Zhang, "A cross-national study of Twitter users' motivations and continuance intentions", Journal of Marketing Communications ahead-of-print, **(2014),** pp. 1-20.
[14] www.fabernovel.com/socialnetworks.pdf.
[15] P.-A. Rutledge, "WordPress on Demand", Que Publishing, privacy in social network sites, **(2013),** wordpress.com/.
[16] J. L.Wayman, "Fundamentals of biometric authentication technologies", Int. J. Image Graph., vol. 1, no. 1, , **(2001)**. pp. 93–113.
[17] http://www.sersc.org/journals/IJUNESST/vol2_no3/2.pdf.
[18] http://www.comp.hkbu.edu.hk/~ycfeng/project/Biometric%20Cryptosystems%20Issues%20and%20Challenges.pdf.
[19] B. K. Bala and J. L. Joanna, "Multi Modal Biometrics using Cryptographic Algorithm", European Journal of Academic Essays, vol. 1, **(2014),** pp. 6-10.
[20] Y. Feng, Y. C., P. C. Yuen and A. K. Jain, "A hybrid approach for face template protection", SPIE Defence and Security Symposium, International Society for Optics and Photonics, **(2008)**.

[21] C. Soutar, D. Roberge, S. A. Stojanov, R. Gilroy and B. K. V. V. Kumar, "Biometric Encryption using Image Processing, Proc. SPIE, Optical Security and Counterfeit Deterrence Techniques II, vol. 3314, **(1998)**, pp. 178-188.
[22] C. Soutar, D. Roberge, S. A. Stojanov, R. Gilroy and B. K. V. V. Kumar, "Biometric Encryption - enrolment and verification Procedures", in Proc. SPIE, Optical Pattern Recognition IX, vol. 3386, **(1998)**, pp. 24-35.
[23] C. Soutar, D. Roberge, S. A. Stojanov, R. Gilroy and B. K. V. V. Kumar, "Biometric Encryption", in ICSA Guide to Cryptography, R. K. Nichols, Ed. New York, McGraw-Hill, chapter 22, **(1998)**.
[24] http://www.biometrics.org/introduction.php.
[25] C. A. Shoniregun and S. Crosier, "Securing biometrics applications", Springer US**, (2008).**

Authors

Shilpi Sharma, she is Assistant Professor and PhD student at Amity University, Uttar Pradesh (Noida), India. Her research interest includes security, privacy, social networks. She has more than 15 years of experience in academics. Mrs. Sharma is member of IEEE, IAENG, and ACM. She is the author/co-author of more than 10 publications in International and National Journals and Conferences.

Dr. JS Sodhi, he is the CIO, Head-IT designated as Assistant Vice President at AKC Data Systems Pvt. Ltd. He received his Doctorate from Amity University in Information Security. He has participated as distinguished Speaker at various National & International Conferences, published in various prestigious journals and given guest lectures to Management students.

