BIOMETRICS SECURITY AND PRIVACY PROTECTION

AHMED A. ASAKER
Reactors Department, Nuclear Research Center – Egyptian Atomic Energy Authority
Cairo, Egypt
Email: ahmad.asaker@gmail.com

OSAMA ZAHRAN
Department of Electronics and Electrical Communication Engineering, Faculty of Electronic Engineering
Menoufia University, Menoufia, Egypt
Email: osama_zahran@el-eng.menofia.edu.eg

Abstract

Physical security at nuclear facilities is an important licensing and design consideration. The ultimate objective of the physical protection system (PPS) is to prevent the accomplishment of unauthorized overt or covert actions to nuclear facilities and nuclear materials. When a physical protection system is applied to a nuclear facility or to nuclear materials, its objective is to prevent radiological sabotage of facilities and theft of nuclear materials. Thus an effective system of physical protection also plays an important role in preventing illicit trafficking of nuclear materials. One of the main pillars of physical protection is controlling personnel access to facilities via Identification technology Systems. Identification technology is changing as fast as the facilities, information, and communication it protects. Recent years have seen a rapid adaptation of using various biometric systems for trusted human automatic recognition and controlling personnel access to nuclear facilities attributed to its high accuracy performance, discriminability, difficulty to be imitated and faked, and stability. Biometrics refers to the physiological or behavioural characteristics of an individual. Many physical characteristics, such as face, fingerprints, iris and behavioural characteristics, such as voice and gait are believed to be unique to an individual. With the exponential growth of using biometric systems, there is an increasing concern that the privacy anonymity of individuals can be compromised by biometric technologies. Unlike passwords and credit cards, which can be revoked and replaced when compromised, biometrics is always associated with a person and cannot be reissued. Biometrics is not secret; the iris of individual can be observed anywhere they look, people leave their fingerprints on everything they touch, and the person will not realize that his/her biometric is disclosed. Biometrics absolutely are sensitive information, therefore biometrics should be protected, because it may be misused by any attacker. To overcome the vulnerabilities of biometric systems, a number of recent strategies can be used such as biometric watermarking, visual cryptography, steganography and cancellable biometrics. In this article, we provide an overview of various methods that used for preserving the privacy and security of the individual's biometrics data.

1. INTRODUCTION

Physical security at nuclear facilities is a vital licensing and design consideration, especially in the light of heightened concerns over terrorist activities following the activities of Sep 11, 2001. Based on the basic IAEA guidance [1-3] to ensure the commitment following the convention on the physical protection of nuclear material, the non-proliferation treaty and the implementation of safeguards, from the start of the operation of nuclear power plants and other nuclear facilities, the physical protection of these nuclear facilities and nuclear materials has been ensured.

One of the main pillars of physical protection is controlling personnel access to facilities via identification technology systems. Identification technology is changing rapidly as the facilities, information, and communication it protects.

Identifying people methods fall into three main categories of increasing reliability and increasing equipment cost as shown in Fig. 1:

i. What you have
ii. What you know
iii. Who you are

What you have; Least reliable (may be shared or stolen): What you have is something you carry such as a key, a card, or a token. It can be also as dumb as an old fashioned metal key or as smart as a card that have a built-in processor that exchanges information with a reader. It can be also in the form of a card that has a magnetic strip that carry information about individual (similar to the familiar ATM card); as well as it can be in the form of a token or card that have a transmitter and/or receiver which have the ability to communicate with the reader from a short distance. This method of identification is the least reliable form of identification, as there is no guarantee that it is being used by the correct person as it may be shared, stolen, or lost and found.

What you know; More reliable (can't be stolen, however it can be shared or written down): What you know is a password or a code. A password/code provides a security problem: if it is simple to remember, then it will probably be easy to estimate; if it is hard to remember, then it will probably be hard to estimate but it will also probably be written down, as a result, security will be reduced. What you know is more reliable than What you have, but passwords and codes can still be shared, as well as if written down they carry the risk of discovery.

Who you are; Most reliable (based on something physically unique to you): Who you are refers to identification via recognition of unique physical characteristics. This is the natural way humans identify one another with nearly total certainty. When accomplished by technological means, it's called biometrics. Biometric scanning technologies had been developed for a number of human features that lend themselves to quantitative analysis.

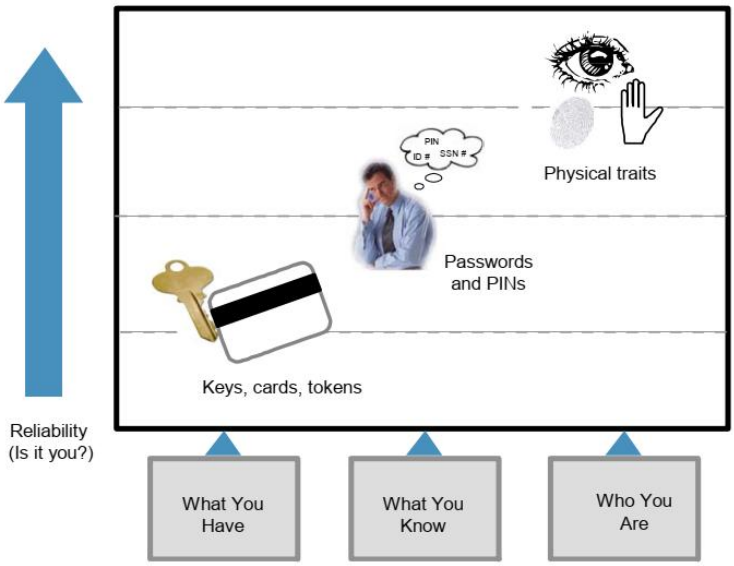

FIG. 1. What You have, What You Know, Who You Are.

Biometric technology is growing fast, getting better and less expensive. Nowadays, many suppliers provide a wide range of biometric devices, as well as, biometrics can be used as a complementary for existing security measures; subsequently biometric technology become best practice for access control when used in combination with traditional "what you have" or "what you know" methods.

Biometric identity is generally used not to recognize identification via searching a database of users for a match, but to confirm identification that is firstly established by a "what you have" or "what you know" method as an instance, a card/PIN is firstly used, then a fingerprint scan confirms the result. As overall performance and confidence in biometric technology growth, it can eventually become a standalone method of identification, without a need for carrying a card or remembering a password.

Regardless of the extensive deployment of biometric technology in diverse applications, the use of biometrics increases different security and privacy concerns as mentioned below [2]:

i. Biometrics is not secret:

The knowledge-based authentication strategies definitely rely on secrecy. For instance, passwords and PINs are recognized only to the user and subsequently secrecy can be achieved. In comparison, biometrics such as face, voice, signature, and fingerprints can be recorded easily and probably misused without the user's knowledge. Voice and face biometrics are vulnerable to being easily captured without the user's consent.

ii. Biometrics cannot be replaced or canceled:

If a biometrics data can be provided by a person who is a one of the enrolled individuals, many biometric security concerns could be different. For instance, authentication systems that use biometrics should not have to deal with spoofed biometrics information as well as replay attacks on biometric systems. If an attacker have the ability to access the biometrics samples and can present them to a system emulating a human presence, then there will be no trust associated with the biometrics. Subsequently, the biometrics has been compromised forever. Passwords and PINs can be easily changed if compromised. As well as, for items such as credit cards and badges that might be stolen, they could be replaced. However, biometrics is always associated with the user and cannot be replaced or cancelled if compromised.

iii. Cross application invariance and cross-matching:

It is highly encouraged for using different passwords and tokens in traditional authentication systems. However, biometrics-based authentication methods depend on the same biometrics. If a biometric template is compromised once, it is exposed forever. If a biometric template is compromised in one application, then the same method can be used for compromising overall applications at which the same biometric is used.

iv. Persistence:

While relative robustness over time is an advantage for biometrics it can also be a massive challenge from a privacy point of view when it requires to be changed. The distinctiveness contained in biometrics is still the same despite the signal as well the template can look different.

Biometrics definitely is sensitive information; therefore biometrics should be secured, because it can be misused by any attacker. Our aim in this article is to survey recent available approaches that used for preserving the privacy and security of the individual's biometrics data.

2. BIOMETRICS SECURITY AND PRIVACY PROTECTION STRATEGIES

2.1 Encryption techniques

One of the earliest techniques for enhancing the privacy of biometric templates was primarily depend on using of encryption techniques such as DES, AES, RSA or ECC encryption. In Cryptography, biometric information is transformed into an unreadable data format as illustrated in Fig.2; subsequently the hacker cannot read it. Transformation process is called encryption. A computational tool is required to perform decryption of the encrypted biometrics data. However, the problem of using this technique is that it makes it possible for the hacker to observe that something fishy is being transmitted. This attracts his interest to try and decrypt it using different ways. Generally, the process of encryption doesn't confine the very existence of the covert data.

Another problem for using the encryption approach for securing biometrics data is that, mostly of encryption algorithms produce a significantly distinct digest even with minor variations in the input. In reality, all biometrics data change with environmental conditions. For example, face and iris biometrics are seriously affected by illumination conditions. Consequently, practically these techniques cannot be used directly in spite of being theoretically extremely strong when applied only to exact data. Moreover, when biometrics data are encrypted, decryption is needed for them to carry out matching. Which creates a potential attack point to get access to the decrypted templates [2, 3].

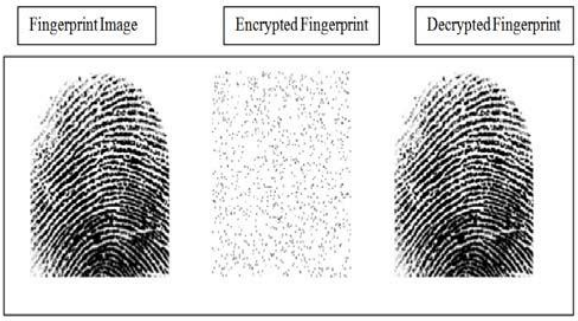

FIG. 2. An example of cryptography carried out in fingerprint biometrics.

2.2 Visual Cryptography Technique

Visual cryptography is a type of cryptography in which the privacy of biometrics data such as face image can be protected by creating a number of shares or transparencies out of the original image by employing decomposition of the image. The decomposed image or shares no longer reveal any information about the original biometric image. The information of the main image can be revealed only when both shares are available at the same time.

During the enrolment process, the private biometrics information is transmitted to a trusted third-party entity. When the biometrics data are received by the trusted entity, it is decomposed into two shares and the original biometric image is discarded. The decomposed components are then sent and stored in two separate database servers such that, the identification of individual's biometrics data is not revealed to either server.

During authentication stage, the trusted entity transmits a request for each server and the corresponding shares are sent to it. Shares are overlaid for reconstructing the original biometric image, avoiding any complication associated with decryption and decoding computations that are used in cryptosystem approaches. The reconstructed image will be discarded once the matching process is achieved. Furthermore, cooperation between the two servers is essential for reconstructing the original biometric image. Fig.3 shows an example of these transformations which carried out in fingerprint biometrics [4, 5].

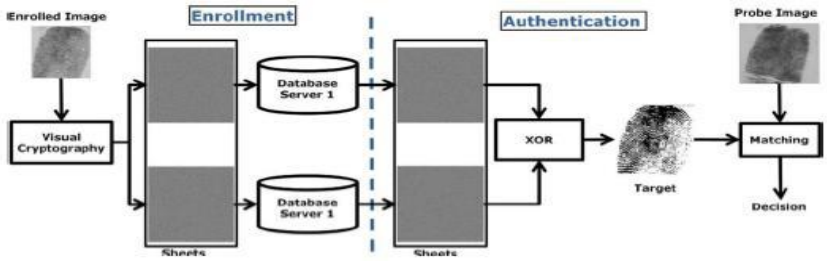

FIG. 3. An example of visual cryptography carried out in fingerprint biometrics

2.3 Biometric Watermarking

Biometric watermarking is another technique for protecting the biometrics data, The concept of watermarking is to introduce some extra information into the biometric features templates leading to a certain distortion to the biometric feature templates. This technique does not introduce any detectable degradation on recognition performance. Additionally, in the case of severe attacks to watermarked image, the recognition performance drops extensively. A biometric watermarking technique for iris recognition was proposed in [6], wherein, the protection of iris templates was carried out via embedding an extra information on the iris image as shown in Fig.4.

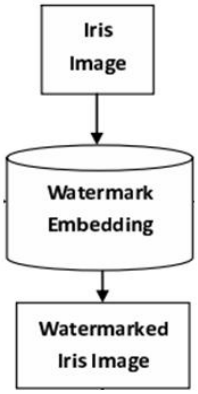

FIG. 4. An example of biometric watermarking applied on iris image.

2.4 Steganography Techniques

Steganography is another approach that can be utilized for avoiding the unauthorized modification of biometrics data. Steganography is the art and technology of invisible communication which is implemented via hiding the biometrics digital data into different type of digital data, hence hiding the existence of the communicated biometrics data for people except the intended individuals will not capable to even guess that there is a covert communication occurring. A successful attack on a system of steganographic consists of an attacker observing that there is hidden information inside a file.

Generally all digital file formats can be utilized as cover objects for steganography, however the digital formats that has a high degree of redundancy such as text, images, Audio, video and protocol are more suitable for steganography. The broadcast of digital images, especially on the Internet, in addition to the large amount of redundant bits present in the digital image representation make images the most popular carriers for steganography among all forms of steganography categories [7, 8].

Fig. 5 shows an instance for a stegnography method applied on finger print. As shown in Fig.5 (a), the simple least significant bit (LSB) steganography approach was applied here for embedding of the fingerprint data into least significant bit on each pixel of the cover image leading to the stego image which clearly looks the same as the cover image. As shown on Fig.5 (b), the extraction manner is exactly the reverse technique of the embedding [9].

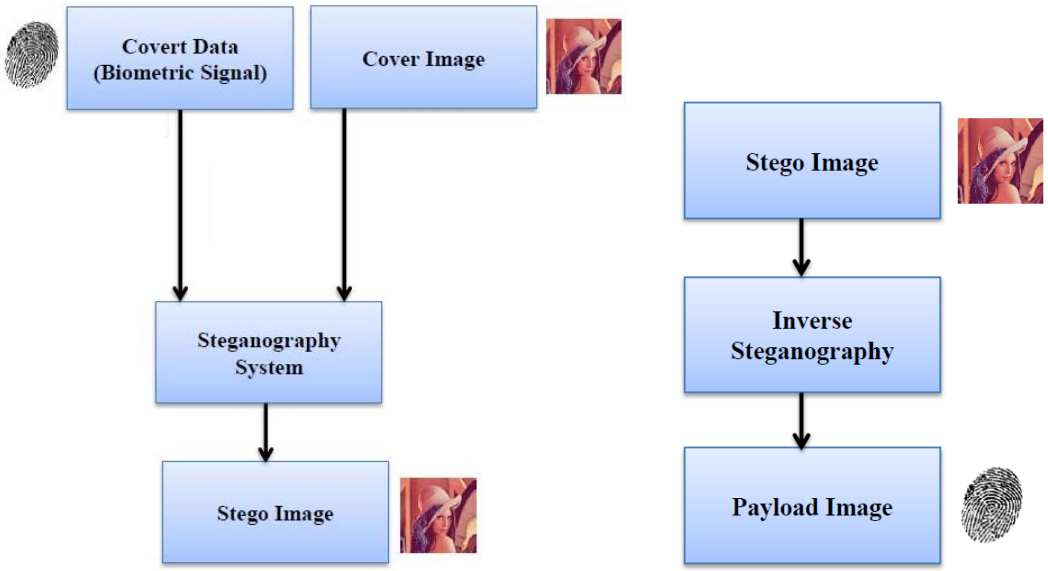

FIG. 5. An example of Steganography model applied on fingerprint
a) Embedding Algorithm b) Extraction Algorithm

2.5 Cancellable biometric

Cancellable biometrics is a new trend that used for more security for biometrics data for individuals. In which, the biometric data is transformed using one-way function then the resultant version of the enrolled biometrics data will be stored in database instead of storing the original biometrics data. The transformation could be carried out directly in the original biometric images or in the feature templates. In case of emergency, the cancellable biometrics can be revoked and reissued simply without a need to change the system at all. Cancellable biometrics is a promising and evolving trend towards more secure biometric systems. Fig. 6 shows the main idea of cancellable biometric applied on feature template using noninvertible transformations [2].

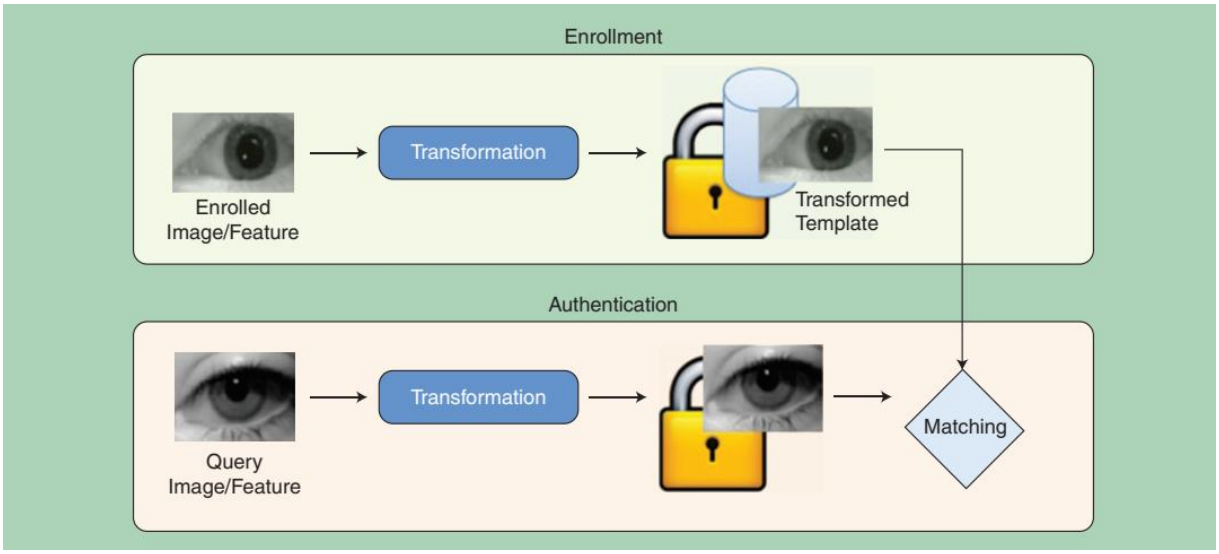

FIG. 6. An example of cancellable biometric system applied on IRIS

An example of a cancellable biometric transformation carried out on Feature-domain for fingerprint biometrics are illustrated in Fig.7. In which, noninvertible transformation function y = f (x) are applied on each minutiae position (feature). The minutiae position x0 is transformed to y0 = f (x0). If y0 is known, the inverse transformation is a many-to-one transformation. x1, x2, x3, x4, x5, x6, x7 are all valid inverse transformation to y0 [10].

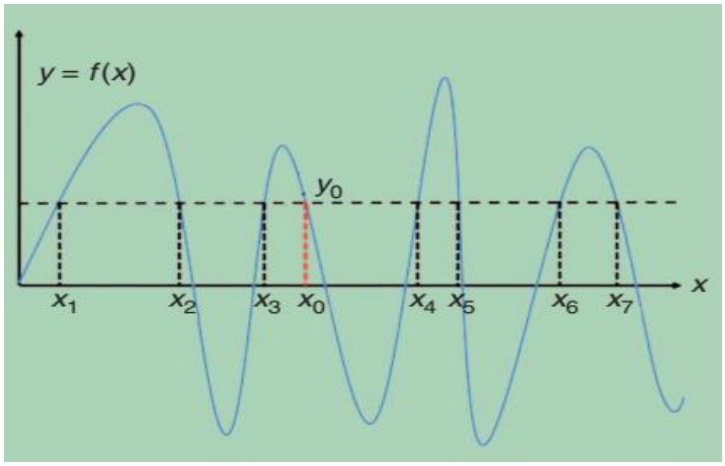

Fig. 7. Feature-domain cancellable biometric transformation for fingerprint biometrics

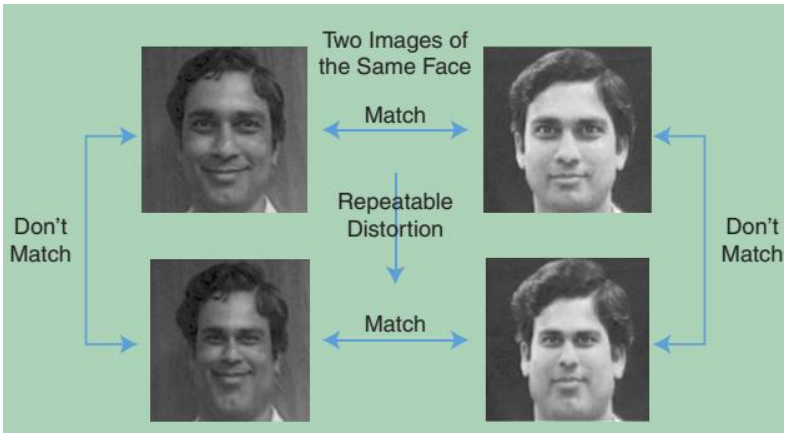

FIG. 8. an example of cancellable biometric transformation applied on original image for face recognition

Another illustration of cancellable biometrics which carried out on original image for face recognition is shown in Fig.8. The face is distorted in the original pixel domain before extracting the feature template. The distorted version does not match with the original face image, while the two distorted faces match among themselves.

2.6 Hybrid methods

Numerous biometric template protection methods use a combination of different technologies. For instant, one hybrid system that uses a combination of visual cryptography and LSB steganography is given in Fig. 9, in which the biometric information is decomposed into two shares, each share was stored in a separate database server such that, the original biometric image can only be revealed when both shares are available at the same time. Subsequently, the identification of the biometrics data cannot be achieved in the absent of either share. Each share was covered with a different cover image selected from a public host image database [11].

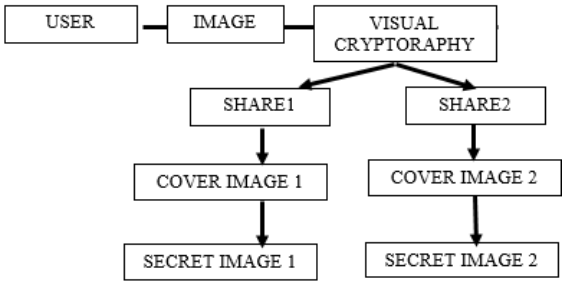

FIG. 9. An example of hybrid method based on a combination of visual cryptography and steganography

In [12], a combination of steganography and watermarking scheme are used for securing the biometrics data which is transmitted over the public networks for personal identity with extra emphasis on iris templates. As shown in Fig. 10, the iris templates was embedded as a watermark, then the watermarked biometric image was embedded on a cover image which was selected from a public host image database to make it more secured and protected against copy attack.

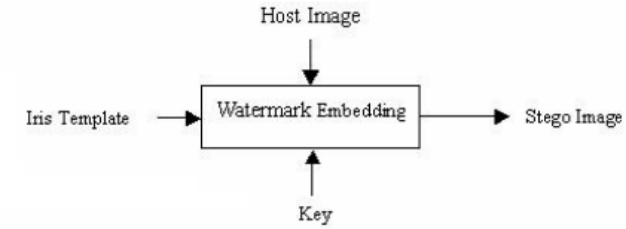

FIG. 10. An example of hybrid method based on a combination of watermarking and steganography

3. Conclusion

Nowadays, biometric technologies provide a reliable solution for identity verification problem that allows restriction access to confidential data via unauthorized users. With the widespread deployment of biometric systems in various applications, there is an increasing concern that biometric technologies can be compromised and misused by any attacker. So, biometrics definitely is sensitive data and therefore it should be properly secured. This article presented a review of recent protection schemes developed for preserving the privacy and security of biometrics data which included encryption techniques, visual cryptography technique, watermarking, stegnography, cancellable biometrics and hybrid methods.

Among different approaches that can be used for preserving the privacy and security of the individual's biometrics data, cancellable biometric scheme has been widely recognized as one of the desirable solutions towards more secure biometrics attributed to its diversity, revocability and non-invertibility. Additionally, cancellable biometric scheme can be combined with other approaches as means of providing improved biometric security and user privacy.

REFERENCES

[1] International Atomic Energy Agency, "Convention on the Physical Protection of Nuclear Material", INFCIRC/274/Rev.1, IAEA, Vienna, May 1980.

[2] Vishal M. Patel, Nalini K. Ratha, and Rama Chellappa, "Cancelable Biometrics", IEEE Signal Processing Magazine, pp. 54-65, September 2015.

[3] Dr M.Gobi and D.Kannan, "A Secured Public Key Cryptosystem for Biometric Encryption" International Journal of Computer Science and Information Technologies, Vol. 5 (1) , pp. 184-191, 2014.

[4] Himanshu Gupta1 and Nupur Sharma, "A Model for Biometric Security Using Visual Cryptography", International Conference on Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions), AIIT, Amity University, Uttar Pradesh, Noida, India, Septemper 7-9, 2016.

[5] Deepak Aeloor and Amrita A. Manjrekar, "Securing Biometric Data with Visual Cryptography and Steganography", International Symposium, SSCC 2013 Mysore, India, Proceedings, Springer-Verlag Berlin Heidelberg, August 2013.

[6] Dong, J., Tan, T., " Effects of Watermarking on Iris Recognition Performance", Proc. 10th Int. Conf. Control, Automation, Robotics and Vision, pp. 1156–1161, 2008.

[7] Stuti Goel, Arun Rana and Manpreet Kaur, "Comparison of Image Steganography Techniques", International Journal of Computers and Distributed Systems, Vol. No.3, Issue I, May 2013.

[8] Shivani Kundra and Nishi Madaan, "A Comparative Study of Image Steganography Techniques", International Journal of Science and Research (IJSR), Volume 3, Issue 4, April 2014.

[9] Srinidhi G A and K B Shiva Kumar, "Secured Biometric Signal Transfer using Steganography", International Journal of Engineering and Technology, July 2017.

[10] N. Ratha, S. Chikkerur, J. Connell, and R. Bolle, "Generating Cancelable Fingerprint Templates", IEEE Trans. Pattern Anal. Mach. Intell., Vol. 29, No. 4, pp. 561–572, April 2007.

[11] Deepak Aeloor and Amrita A. Manjrekar, "Securing Biometric Data with Visual Cryptography and Steganography", Springer-Verlag Berlin Heidelberg, August 2013.

[12] Muhammad Khurram Khan, Jiashu Zhang, and Lei Tian, "Protecting Biometric Data for Personal Identification", Springer-Verlag Berlin Heidelberg, 2004.