AUTHENTICATION BASED ON FINGERPRINTS WITH STEGANOGRAPHIC DATA PROTECTION

Narek Malkhasyan

Abstract: *This paper examines security problems of biometric based authentication. An authentication method is suggested, which is based on fingerprints with steganographic data protection in all stages of functioning. Suggested procedures of fingerprint based enrollment and authentication are also functionally described.*

Introduction

The increasing computerization of society, together with the prevalence of the internet and "cloud" technologies leads to the fact that both organizations and individuals increasingly rely on modern informational tools. The increasingly complex IT infrastructure of enterprises and organizations, along with the changing nature of the threats and risks make information security a vital issue. However, quite different and effective information security methods can be practically useless if they are not reinforced by convenient and reliable means of authentication (identity establishment) of consumers of information services.

Recent years are characterized by steady increase in interest in biometric authentication methods, which are based on physiological and behavioral characteristics of the user, and which are far better than traditional means, such as passwords, ID cards, etc.One main reason for this popularity is the ability of biometric technology to relatively simply and easily distinguish legitimate users from hackers attempting to fraudulently obtain access rights to information resources[1, 2]. Currently the most common are the technologies based on fingerprint,as these are the most convenient to use and the most cost-effective. Although, it should be noted that the results for fingerprints are mostly applicable in other biometric systems after undergoing some minor customizations.

At the same time, an analysis of possible attacks on the authentication system based on fingerprints shows that one of the major challenges is to ensure the security and integrity of biometric data[3]. It's obvious that the biometric data, having a high degree of uniqueness, in practice are poorly protected against copying, misuse or modification. Essentially a biometric authentication system can work properly only if it is able to ensure that duringenrollment and authentication data have been received from the relevant user and have not been subjected to external influence[4].Therefore, from the point of view of facilitating widespread usage of biometric methods,the task of protecting biometric data, in particular fingerprint data becomes critical.

Fingerprint protection

Fingerprint security can be achieved through the use of cryptographic techniques. Cryptography can be used for encrypting the fingerprint after scanning to ensure the safe transfer and storage. At the authentication stage both stored during the enrollment and received by the server fingerprint data are being deciphered for the matching procedure. The result is the security of fingerprint data, as it cannot be used or modified without the correct decryption with the corresponding private key. In general, cryptography can be used also to monitor the integrity of the fingerprint to confirm the authenticity of the source.

It should be mentioned that in many security applications biometric information is used to generate passwords for protecting cryptographic keys. A good survey on this problem can be found in [5]. In applications like the one described above it is critical to protect biometric information especially when it is transmitted remotely through an insecure channel.

The implementation of the mentioned protection of biometric data through the use of steganographic techniques [6] seems to befairly promising. While cryptography is primarily focused on techniques designed to make the encrypted information meaningless to outsiders, steganography is based on the concealment of the fact of the existence of secret information. As a result steganographic techniques can be used to protect the fingerprint with the same success providing both security and integrity of data transmitted from the client to the server or stored on the server. This significantly reduces the chance of unauthorized acquisition of biometric data, thus reducing the likelihood of misuse or alteration.

In order to monitor the integrity and authenticity of the fingerprint data source, steganography can be used to embed special labels in the image, often called digital watermarks. The mentioned labels can be embedded both assymbolic and graphic information. In the process of authentication labelsembedded in the fingerprint image can be extracted and used to verify the integrity and authenticity. Also the same steganographic techniques can be used for protecting fingerprint images by embedding them in other, not suspicious objects (such as images) often called containers. In other words, we can consider two main areas of steganographic protection of fingerprint data:

- embedding of special labels into fingerprint image for integrity monitoring,
- embeddingof fingerprint images into other images for more secure communication.

Authentication Method

Acombination of these approaches to the steganographic protection is proposed for comprehensive protection of fingerprint data. At first identification labels will be embedded into the fingerprint image, and thenit will be embedded into the container for secure communication. In the general case, the authentication is preceded by user enrollment process, during which the user data is recorded on the server side, and entered into the appropriate storage [7]. Functional scheme of the proposed enrollment process is shown in Figure 1.

User enrollment is carried out in the following order:

- Images of user’s two different fingers are acquired using a suitable scanner, the first of which will then be used for authentication and the second one will be used for integrity control.
- An image is chosen from an archive stored in the user’s computer, which will be used as a container.
- Both scanned fingerprint images are embedded into the container using appropriate steganographic algorithm and key.
- The filled container together with the user ID (name, nickname, password ...)is sent to the server side.
- The resulting filled container with the appropriate user ID is stored in the storage of fingerprints on the server side.

In this procedure, any image file (photo, drawing ...) stored on the computer and having a suitable format for the selected steganographic algorithm can be used as a container. Corresponding selection of steganographic algorithm and a secret key can provide a high level of protection of the fingerprint data during transmission and storage on the server. Other files supported by the selected steganographic algorithm, can also be used as a container in the mentioned scheme (audio, video ...) [6]. It should be noted that the enrollment procedure of a user is carried out not often, usually only once, therefore, to provide a high level of security it is quite permissible to use full-sized fingerprint images and large steganography container files.

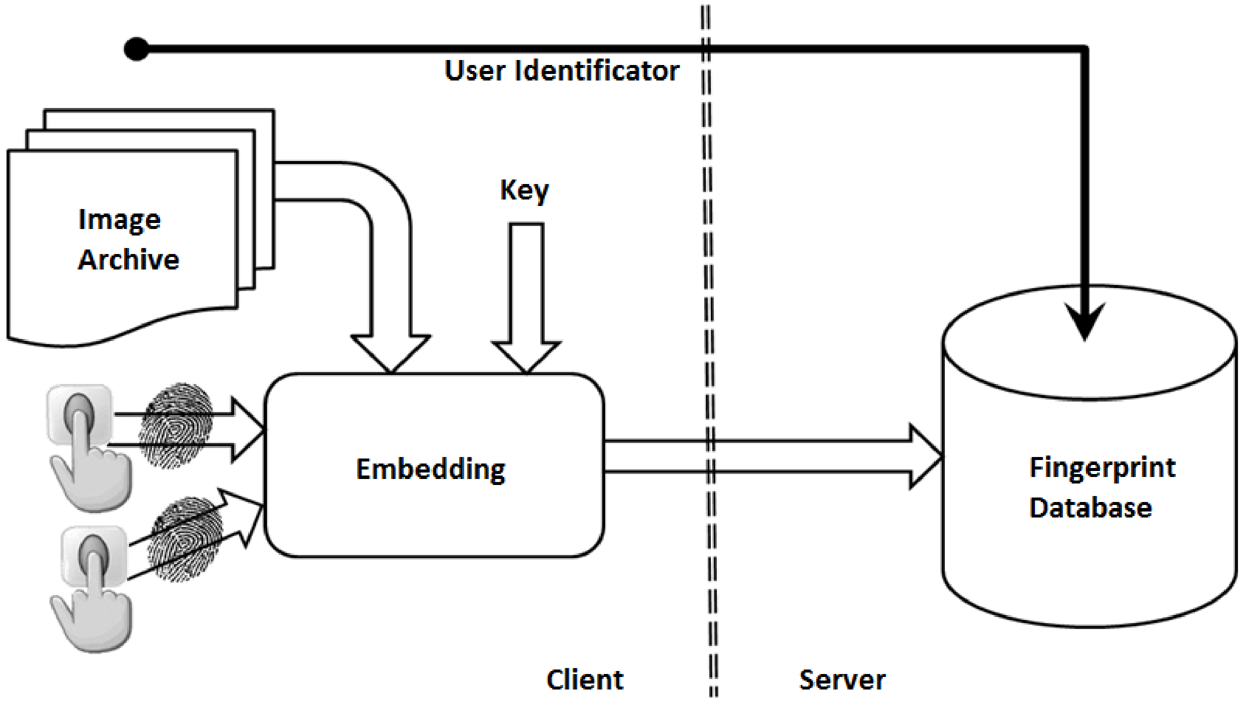

Figure 1. Functional Scheme of User Registration Procedure

Obviously, during the authentication stage the same fingers of the user should be scanned and securely transmitted to the server. To provide a higher level of secrecy of the data transmission it is possible to use synthetic or real image of some fingerprint as a container. This image is not really involved in the authentication and only distracts the attention of potential adversary who can intercept the information passed through an open channel. At the same time it is necessary to consider that from security perspective, the amount of embedded information should be much smaller than the volume of the container[8]. Therefore, it is proposed to extract a fragment from the first fingerprint image, which has suitable dimensions for embedding, and yet contains sufficient information for authentication. Additionally it is proposed to use minutiae points extracted from the second fingerprint image as a digital watermark, which must be embedded into the first fingerprint image to ensure the authenticity of the fingerprint data source. Based on the above an authentication procedure with steganographic data protection is proposed. The functional diagram of operations of the proposed procedure is shown in Figure 2.

Preparation of information required for authentication is carried out in the following order:

- Two fingers of the user, which have been used at the enrollment stage, are scanned using a suitable scanner.
- A fingerprint image is selected from an archive stored on the user's computer, which will be used as a container.
- A fragment of necessary size is extracted from the first fingerprint image in accordance with the volume of the selected container.
- Minutiae points are extracted from the second fingerprint image.
- The minutiae points’ parameters extracted from the second fingerprint image are embedded into the extracted fragment of the first fingerprint image as a digital watermark using appropriate steganographic algorithm and key.
- The fragment of first fingerprint image is embedded into the container using appropriate steganographic algorithm and key.
- The filled container together with the user ID is passed to the server.

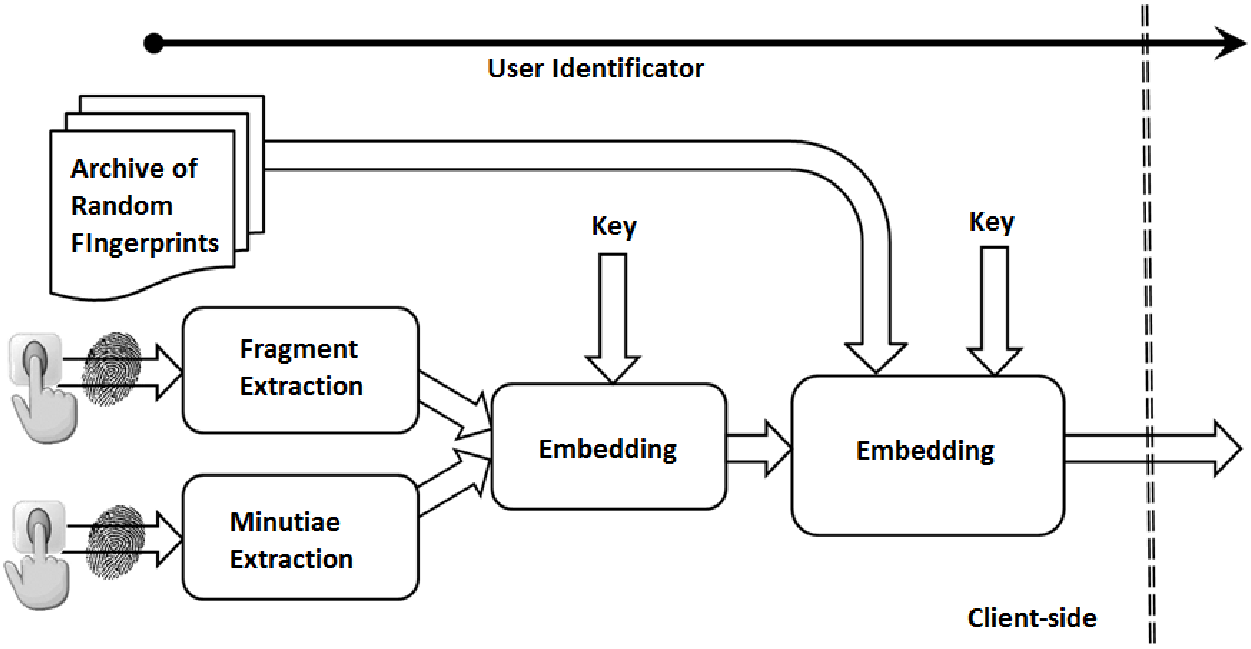

Figure 2. Functional Scheme of Client Side User Authentication Procedure

The functional scheme of the operations of the proposed authentication procedure on the server-side is shown in Figure 3.

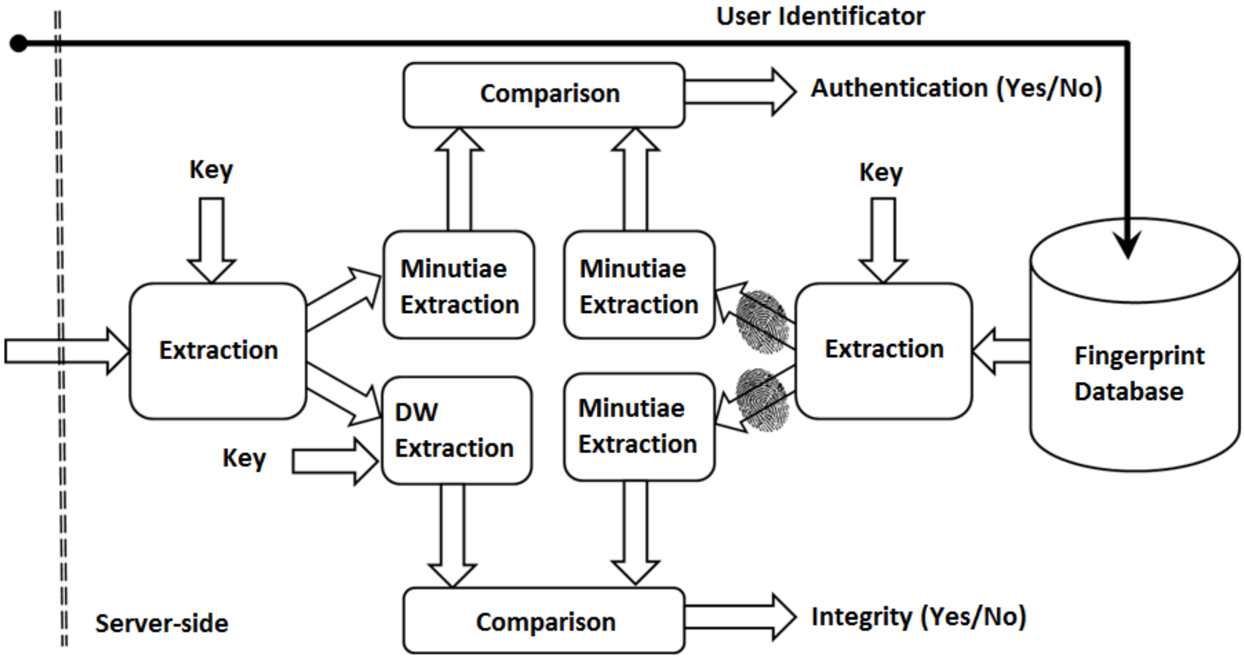

Figure 3. Functional Scheme of Server Side User Authentication

Processing of thereceived information needed for authentication on the server side is carried out in the following order:

- A filled container from the server side storage of fingerprints is retrieved according to the received user ID.

- Two embedded fingerprint images are extracted from the container using appropriate steganographic algorithm and key.
- Minutiae points are extracted from these fingerprint images.
- The fingerprint image fragment is extracted from the received container using appropriate steganographic algorithm and key.
- Using appropriate steganographic algorithm and key the digital watermark is extracted from the fingerprint image fragment, which is a set of parameters of minutiae points of the second fingerprint.
- Minutiae points' parameters extracted from the second fingerprint image, which has been retrieved from storage, are compared with the extracted digital watermark data and a decision regarding the integrity of the received fragment is made.
- Minutiae points are extracted from the extracted fingerprint image fragment.
- Minutiae points' parameters extracted from the first fingerprint image, which has been retrieved from storage, are compared with the minutiae points' parameters extracted from the received fragment and a decision regarding the user authenticity is made.

It should be noted that the same key should be used for embedding into the containers and extracting from them fingerprint images and digital watermarks in all phases of authentication. This key may be agreed between the user and the server as a part of the communication protocol. For safety reasons, different keys can be used for each embedding/extraction operation, which obviously will significantly increase the level of protection, but also will significantly complicate the protocols and procedures.

Security Considerations

Although the fingerprint recognition technique is the dominant technology in the biometric market, it may suffer attacks at different points during the authentication process. The most common attacks occur by the use of fake fingerprint images. These fake fingerprint images can be acquired from different surfaces touched by the legitimate user (such as glasses, doorknobs, glossy paper, etc.) The vulnerability to this kind of attacks has always been considered as a major drawback of fingerprint-based authentication systems.

The suggested method alleviates the mentioned vulnerability to some extent. Let us consider the security of the system from the perspective of an attacker who has access to the communication channel between the client and server modules of the proposed method and who has illegitimately acquired the fingerprint image of a legitimate user of the system. Also let us assume that the attacker has somehow managed to break the steganographic algorithm used to embed fingerprint images into a container, although this task is very hard to accomplish on it's own in the case of appropriate steganographic algorithm selection. In order to pass successful authentication on behalf of the legitimate user the attacker has to take the following additional steps:

- guess the necessity of embedded digital watermark in the fingerprint image,
- acquire the minutiae points of the fingerprint image of the legitimate user's second finger, which obviously is a harder task than acquiring just the fingerprint image from some surface touched by the user,
- break the digital watermark algorithm in order to embed the acquired minutiae points into the fingerprint image of the user's first finger, which, in the case of appropriate algorithm selection, is a very hard task also.

Thus, we can conclude that the proposed scheme adds an additional security layer to the fingerprint authentication process.

Conclusion

The proposed method represented in this paper provides security and integrity of transmitted and stored fingerprint data through the use of steganographic data protection methods. A slight modification of this method can provide its applicability to the problem of identification of registered users.

As a suggestion for a future research in this area the following directionscould be pointed out:

- Development of steganographic algorithms specifically adopted for effective embedding of fingerprint images into containers.
- Development of methodology for extracting fingerprint image fragments of needed size,sufficient for successful authentication.

References

1. A. K. Jain, A. A. Ross,K.Nandakumar, *Introduction to Biometrics*, Springer, 2011, 311 p.
2. L. O'Gorman, *Comparing Passwords, Tokens, and Biometrics for User Authentication*. Proc. IEEE, vol. 91, no. 12, 2003, pp. 2021–2040
3. J. Galbally, J. Fierrez, F. Alonso–Fernandez,M. Martinez–Diaz,*Evaluation of Direct Attacks to Fingerprint Verification Systems*, Telecommunication Systems (Springer), Volume 47, Numbers 3–4, 2011, pp. 243–254
4. B. Schneier, *The Uses and Abuses of Biometrics*, Communications of the ACM, vol. 42, no. 8, 1999, p. 136
5. G. Khachatrian, N. Malkhasyan, Overview of Methods of Biometric Based Key Protection, 2012
6. E. Cole, *Hiding in Plain Sight: Steganography and the Art of Covert Communication*,John Wiley & Sons, 2003. 360 p.
7. D. Maltoni, D. Maio, A. K. Jain, S.Prabhakar, *Handbook of Fingerprint Recognition (Second Edition)*, Springer, 2009, 348 p.
8. 8. G.Margarov, *Data Hiding on the Internet: Steganalysis against Steganography*, in "Terrorism and the Internet – Threats – Target groups – Deradicalisation strategies", IOS Press, 2010, pp. 167–182

Authors information

Narek Malkhasyan - *Institute for Informatics and Automation Problems, National Academy of Sciences of Armenia*