Secure and Privacy Preserving Biometric Authentication Using Watermarking Technique

Doyel Pal[1(✉)], Praveenkumar Khethavath[2], Johnson P. Thomas[1], and Tingting Chen[3]

[1] Computer Science Department, Oklahoma State University, Stillwater, OK, USA
{doyelp, jpt}@cs.okstate.edu
[2] Mathematics, Engineering and Computer Science Department, LaGuardia Community College, CUNY, Longisland City, NY, USA
pkhethavath@lagcc.cuny.edu
[3] Computer Science Department, California State Polytechnic University, Pomona, CA, USA
tingtingchen@csupomona.edu

Abstract. Biometric authentication ensures user identity by means of users' biometric traits. Though biometrics is unique and secure, it can be still stolen or misused by any adversary. In this paper we propose a secure and privacy preserving biometric authentication scheme using watermarking technique. Watermarking is used for content authentication, copyright management, tamper detection, etc. We watermark the user's face image with finger print and encrypt the watermarked biometric to protect its privacy from adversary. The watermarked biometric technique has been used for privacy preserving authentication purpose. The analysis proves the correctness, privacy and efficiency of our scheme.

Keywords: Watermark · Biometric · Authentication · Secure · Privacy – preserving

1 Introduction

Authentication plays an important role to identify or authenticate any user. Authentication is primarily based on what user knows (e.g., password, PIN, etc.) or what user has (e.g., token, chip card, etc.) which can be disclosed, stolen, forgotten or lost. Biometric authentication is a secure way to authenticate any user since it is related to the uniqueness of what a user is, i.e. the physiological or behavioral characteristics of a user (e.g., finger print, iris, face image, handwriting etc.). Though biometric traits are unique and secure, unimodal biometric authentications that uses single biometric trait have some limitations [1, 8]. It is vulnerable to spoof attacks, noise in sensed data, distinctiveness, nonuniversality etc. One way to overcome the limitation is using more than one biometric traits of a user. In this paper we propose a secure and privacy

J.H. Abawajy et al. (Eds): SSCC 2015, CCIS 536, pp. 146–156, 2015.
DOI: 10.1007/978-3-319-22915-7_14

preserving biometric authentication scheme which uses more than one biometric trait that are, face image and finger print using watermarking technique.

Watermarking is a technique to embed specific data in a digital content. Watermarking scheme has enormous diversity. It can be categorized [9–11] based on embedding domain (Spatial domain, Transform domain, Feature domain), watermarking host signal (video signal, audio signal, IC design, etc.), availability of original signal during extraction (blind, semi–blind, non–blind) etc. The watermarking technique is advantageous because, to embed the watermark into the original data this technique does not create any separate file to store authentication information. Besides all the advantages of the watermarking technique, any modification on the embedded data can be manipulated easily. Therefore one important requirement of the watermark technique is to make it almost unrecognizable and robust so that watermark cannot be removed or modified by any attack.

To make the biometric watermarking technique more secure, encryption based privacy preserving techniques can be applied. Though watermarked biometrics is difficult to steal or forge but it is not secure when attacked by any determined attacker [2]. Few watermarking techniques (e.g., fragile, robust) becomes invalid or detectable if a slight modification or some image processing operations such as image scaling, cropping, bending is done on the watermarked image. As any individual's biometric features are unique therefore these biometric features should not be compromised or disclosed under any circumstances to any adversary. In this proposal we focus on the privacy preserving secure biometric watermarking scheme for authentication purpose. We preserve the privacy of users' watermarked biometrics using cryptography. To overcome the vulnerability of biometric authentications and to protect the privacy of user's watermarked biometrics, we use biometric authentication in conjunction with digital watermarking and cryptography. We embed the fingerprint on facial image as watermark to improve the security of user authentication and to achieve the privacy of users' biometric traits we encrypt the watermarked biometric before user verification.

The rest of the paper is organized as follows. In Sect. 2 we discuss about the existing related work. We describe the problem statement and preliminaries in Sects. 3 and 4 respectively. In Sect. 5 we explain the proposed solution. We discuss the system analysis and experimental analysis in Sects. 6 and 7 respectively. In Sect. 8 we give the conclusion.

2 Related Work

To authenticate the identity of any user biometric authentication is one of the most trustworthy techniques as it involves verification of users' biometric traits. Biometric authentication systems authenticate any user based on their physical traits, such as, fingerprint, face image, iris, signature etc. which are unique. Different biometric authentication mechanism has been used extensively in various domains. In [3] the authors proposed a framework for three – factor authentication scheme in a distributed system. A template protecting biometric authentication scheme to fingerprint data has been implemented in [4]. In this finger print based authentication mechanism the

authors have presented an algorithm which identifies the reliable components of Gabor filtered fingerprint and applies quantization to make a binary representation of the fingerprint. Noise correction has been applied on the quantized binary representation. A multimodal biometric authentication scheme for adapting score–level fusion functions based on quality measures has been proposed in [5]. In [6] a novel and efficient facial image representation based on local binary pattern (LBP) has been proposed which extracts the LBP feature distributions by dividing the face image into several regions and concatenates them into an enhanced feature vector to be used as a face descriptor. Instead of using two different biometric traits a personal identification scheme using palm print and hand geometry which can be acquired from the same image has been proposed in [7]. The authors have integrated the hand geometry on the palm print to improve the performance of the verification system.

Ample of biometric watermarking techniques has been proposed. In [9] the authors proposed a semi – blind biometric watermarking scheme using both watermarking technique and face image recognition. The face features are embedded in the non-overlapping blocks of host image using Singular Value Decomposition (SVD). A robust hybrid biometric watermarking approach for offline handwritten signature has been proposed in [10]. The authors amalgamate the lifting wavelet transform (LWT) and SVD to make the biometric watermarking technique robust. In [11] a watermarking scheme in spatial domain for color image using SVD technique has been introduced. Three dimensions of color iris images are used to embed into color face image to make the technique robust and reliable. An image ownership and tampering authentication scheme based on watermarking techniques has been proposed in [12]. The watermarking technique is used here to detect the malicious manipulation over embedded images and to protect the rightful ownership. In [13] the authors proposed an efficient and secure encryption scheme to transmit the biometric data over unsecured data channel. An asymmetric watermarking technique has been proposed in [18]. In [19] a layered architecture for watermarking technique has been proposed which provides security by using cryptography primitive on top of the watermarking algorithm.

3 Problem Statement

In this paper, we verify the authentication of a user in a privacy preserving secure manner using user's biometrics, watermarking scheme and cryptography. The problem can be framed formally as follows. There are n number of users $U_1, U_2, \ldots, U_i, \ldots, U_n$ and a server S which holds a database D_{fv} with all users' encrypted watermarked feature vector $WSDB_{fv}$. Given a user $U_i's$ biometrics, i.e., face image (I) and fingerprint (F), the user's face image $'I'$ will be watermarked with fingerprint $'F'$ and will be denoted as WB_{fv}. The Euclidean distance ∂ between the user's encrypted watermarked feature vectorWB_{fv} and the encrypted watermarked feature vectors $WSDB_{fv}$, in D_{fv} decides the user's authentication (Eq. 1).

$$\partial(E(WB_{fv}), E(WSDB_{fv})) \leq \tau \ldots\ldots \quad (1)$$

τ denotes the threshold value and if $\partial \leq \tau$, the algorithm determines that user is an authentic one.

4 Preliminaries

4.1 Homomorphic Encryption

In this paper we calculate the Euclidean distance between two cipher texts and to do that we use homomorphic property based encryption scheme. Homomorphic encryption technique allows specific types of arithmetic computations on cipher text and when decrypted the plaintext matches with the result of arithmetic operations on plaintexts without seemingly inherent loss of the encryption. In ring theory, homomorphism is a mapping $\varphi : R \rightarrow S$ that respects both addition and multiplication. Therefore,

$$\forall x, y \in R, \quad \varphi(x + y) = \varphi(x) + \varphi(y) \; and \; \varphi(xy) = \varphi(x)\, \varphi(y)$$

The homomorphic encryption which preserves a single operation such as addition or multiplication is known as partially homomorphic encryption and those which preserves both of the addition and multiplication is known as fully homomorphic encryption. For example, RSA and ElGamal [14, 15] supports the multiplicative homomorphic property, i.e., if $E(x)$ denotes the ciphertext of plain text x then according to multiplicative homomorphism,

$$E(x_1) \cdot E(x_2) = E(x_1 \cdot x_2)$$

Whereas the additive homomorphic property of Paillier cryptosystem [16] denotes that,

$$E(x_1) \cdot E(x_2) = E(x_1 + x_2)$$

4.2 Singular Value Decomposition

In Linear Algebra, Singular Value Decomposition [17] is a factorization technique of a real or complex matrix. In signal processing SVD has been used in applications, e.g., watermarking, noise reduction, image compression, etc. According to SVD theorem any rectangular matrix A of m $\times$ n dimension can be decomposed into the product of three matrices: an orthogonal matrix U of size m $\times$ m, a diagonal matrix S of size m $\times$ n and the transpose of a orthogonal matrix V of sizen $\times$ n.

$$A_{m \times n} = U_{m \times m} S_{m \times n} V_{n \times n}$$

The original matrix can be obtained by multiplying U, S, V^T.

$$A = U_{m\times m} S_{m\times n} V^{T}_{n\times n}$$

SVD based watermarking techniques can be categorized into many categories [9], such as, by modification right/left singular vectors of the host images, modification of all singular vectors, hybrid transformation techniques which combines SVD with other transformations(DWT, DFT, DCT, etc.), etc.

5 Proposed Solution

We propose a solution for privacy preserving secure biometric authentication scheme using watermarking technique in this paper. We consider two biometric traits, face image (I) and fingerprint (F) for biometric watermarking authentication purpose and extract the feature vectors from both of these biometrics. To make the entire authentication procedure secure we perform some specific transformations on the real biometric feature vectors instead of using the original biometric feature vectors. The reason behind distorting the feature vectors is to make the authentication more secure. So even if any adversary manages to get the water marked feature vector, they will not be able to get the transformed matrices to be worked on. Since nowadays anyone's face image can be captured by any adversary we will watermark the transformed face image with transformed finger print image to make it more secure. We use linear transformation, i.e., rotation on the actual feature vectors and denote it as transformed feature vector afterwards in this paper. We watermark the transformed feature vector of face image (TSI) with transformed feature vector of fingerprint (TSF) using SVD based watermarking technique. On the watermarked biometric we perform all the further computation for authentication. The watermarked feature vector is stored in the server to authenticate any user. To preserve the privacy of user's watermarked biometrics we encrypt the watermarked biometrics using homomorphic encryption scheme at both the server end and user end. A user is authenticated by calculating the Euclidean distance

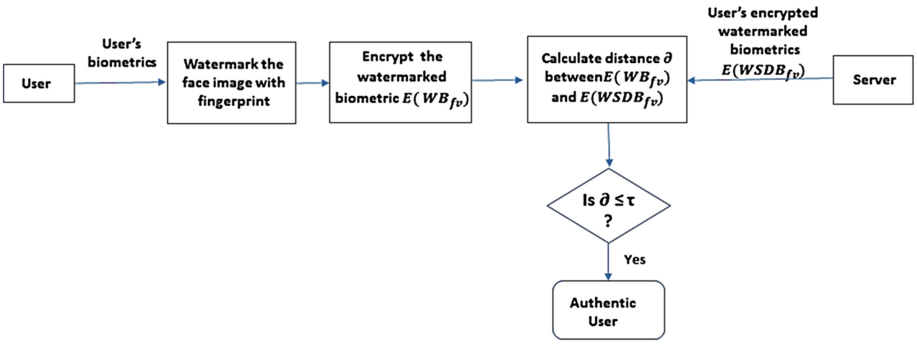

Fig. 1. Overall flow of the authentication mechanism

between the encrypted watermarked biometric provided from user end and the encrypted watermarked biometric from server end. Since Euclidean distance between cipher texts will be calculated we use one of the homomorphic encryption techniques as it allows computation on cipher texts. The distance less than some threshold value τ indicates that the user is an authenticate one. The overall flow of the entire authentication procedure is given in Fig. 1 below.

Algorithm 1

Input: User's finger print F, user's face image I

Steps:

1. The system generates private key – public key pair (x, y) where x is the private key and y is the public key.
2. The server S keeps a database DB for all users water marked biometrics $WSDB_{fv}$
3. Get the feature vector matrix F_{fv} of finger print F.
4. Get the feature vector matrix I_{fv} of face image I.
5. Perform rotation on face image feature vector, $RI_{fv} = \text{Rotation}(F_{fv})$
6. Perform rotation on finger print feature vector, $RF_{fv} = \text{Rotation}(I_{fv})$
7. Perform SVD based watermarking method to watermark RI_{fv} withRF_{fv}. The resulting biometric for user U_i becomes WB_{fv}
8. $for\ i = to\ n$
9. $for\ j = to\ m$
    a. Compute $E(g^{WB_{fv}[i,j]})$and $E(g^{WB_{fv}[i,j]^2})$ and sends them to the server.
10. $end\ for$
11. $end\ for$
12. Server computes
$$C = \prod_{i,j=1}^{m,n} E(g^{WB_{fv}([i,j]^2)})\, E(g^{WB_{fv}[i,j]})^{-2(WSDB_{fv}[i,j]} E(g^{WSDB_{fv}[i,j]^2})$$
13. Server decrypts C with private key x and obtain
$$D(C) = g^{\sum_{i,j=1}^{m,n}(WB_{fv}[i,j] - WSDB_{fv}[i,j])^2}$$
14. $if\ D(C) \leq \tau$
    The user is authenticated.
15. $else$
    Discard the user
16. $end\ if$

5.1 Algorithm

In this section we describe the algorithm (Algorithm 1) for the proposed solution. At first the feature vectors of user's face image and finger print will be extracted. The feature vectors will be distorted using some linear transformation, e.g., rotation

(Algorithm 1 line 4–5). To watermark the transformed face image, RI_{fv} with transformed finger print, RF_{fv} we use SVD based watermarking technique [21] (Algorithm 1 line 6). The rest of the computations will be performed on watermarked feature vector WB_{fv}.

We use the ElGamal encryption scheme to encrypt the watermarked feature vectorWB_{fv}. Algorithm 1 at the user end computes $E(g^{WB_{fv}[i,j]})$ and $E(g^{WB_{fv}[i,j]^2})$ and sends them to the server (line 7–10). The server has the watermarked transformed feature vector for all users beforehand. To check the authentication the server computes the Euclidean distance between the encrypted feature vectors $WSDB_{fv}$ and WB_{fv} for a particular user (Algorithm 1 line 11). The server computes

$$C = \prod_{i,j=1}^{m,n} E(g^{WB_{fv}([i,j]^2)}) E(g^{WB_{fv}[i,j]})^{-2(WSDB_{fv}[i,j]} E(g^{WSDB_{fv}[i,j]^2})$$

which is the Euclidean distance between the encrypted feature vectors. The decrypted Euclidean distance $D(C) = \partial \leq \tau$ denotes that the user is an authenticate one.

6 System Analysis

In this section we analyze the proposed solution in terms of correctness, privacy and performance.

6.1 Correctness Analysis

To proof the correctness of Algorithm 1 it should be proved that server and the user computes the Euclidean distance without knowing the plain text of the feature vectors. The line number 13 of Algorithm 1 can be proved by the homomorphic property of ElGamal algorithm. Figure 2 depicts the correctness of our algorithm.

6.2 Privacy Analysis

In this section we will discuss about the privacy of the proposed solution. We assume that the server is secure. Algorithm 1 is secure in a semi honest model [23]. The user sends the encrypted biometrics to server therefore any adversary will learn nothing but the encrypted watermarked feature vector. Moreover the server does the computation on the cipher texts to get the distance, which implies that Algorithm 1 is secure in a semi honest model. The only decrypted text is the encrypted distance from which no one can learn about the user's biometrics which indicates privacy is preserved in our proposed solution.

$$
\begin{aligned}
& D(C) \\
&= D\Big(\prod_{i,j=1}^{m,n} E\big(g^{WB_{fv}([i,j]^2)}\big)\, E\big(g^{WB_{fv}[i,j]}\big)^{-2(WSDB_{fv}[i,j])} E\big(g^{WSDB_{fv}[i,j]^2}\big)\Big) \\
&= D\Big(E\Big(\prod_{i,j=1}^{m,n} g^{(WB_{fv}([i,j])^2}\, g^{(WSDB_{fv}[i,j])^2)}\Big) \prod_{i,j=1}^{m,n} \big(E\big(g^{(WB_{fv}[i,j])}\big)^{-2\left(WSDB_{fv}[i,j]\right)}\big)\Big) \\
&= D\Big(E\Big(\prod_{i,j=1}^{m,n} g^{(WB_{fv}([i,j])^2}\, g^{(WSDB_{fv}[i,j])^2} g^{(WB_{fv}[i,j])^{-2(WSDB_{fv})}}\Big)\Big) \\
&= D\left(E\left(g^{\sum_{i,j=1}^{m,n}\left(WB_{fv}[i,j]-\, WSDB_{fv}[i,j]\right)^2}\right)\right) \\
&= g^{\sum_{i,j=1}^{m,n}\left(WB_{fv}[i,j]-\, WSDB_{fv}[i,j]\right)^2}
\end{aligned}
$$

Fig. 2. Correctness analysis

7 Experimental Analysis

7.1 Experiment Setup

To test the performance we consider different face images sizes varying from 3 KB–7 KB and embed different finger prints on them using watermarking technique. Before watermarking the face image we extract the feature vectors of face image and finger print and transform them by linear transformation technique. To extract the feature vector of biometrics we use PCA - based Face Recognition System package using Matlab [20]. For watermarking purpose, we use the SVD based watermarking technique proposed in [21]. To implement our technique we use the Java programming language and JAMA package [22], since feature vector comes as a form of matrix. We use the SVD based watermarking technique, but because of the constraint of JAMA package for SVD calculation we modified the library so that it can work for any type of feature vector matrix. Existing JAMA package works correctly only for full rank $m \times n$ matrices with $m \geq n$.

7.2 Performance Analysis

We evaluate the performance of our technique in terms of time for different modules that are, watermarking time, encryption time and distance calculation time.

Figure 3 shows the computation time to watermark the face image with finger print image using SVD based watermarking technique at the user end for different file sizes. We vary the file sizes from 10 KB to 100 KB with 10–20 KB interval. Figure 3 shows that if we increase the face image size then the time to watermark the biometrics increases linearly.

We encrypt the watermarked face image with ElGamal encryption technique. Figure 4 depicts the time to encrypt the watermarked feature vector at the user end for different size of face images. The time to encrypt the watermarked face images increases linearly with the increasing face image sizes.

The user is an authenticate one if the distance between the encrypted watermarked biometric at the user end and at the server end is below some threshold value τ.

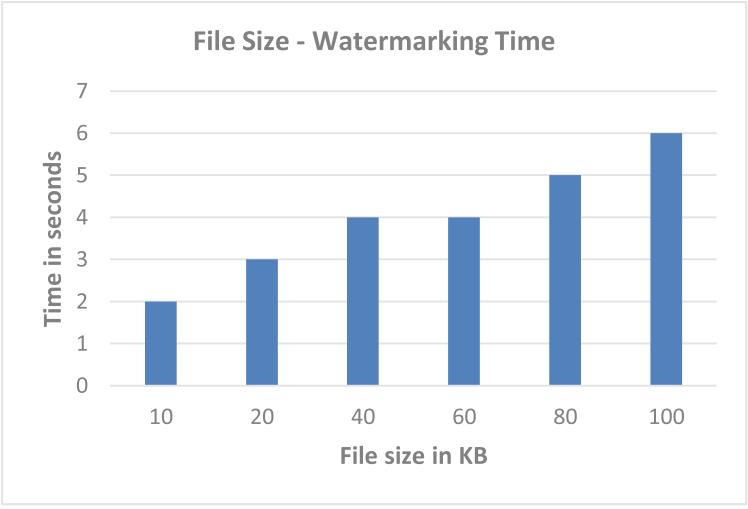

Fig. 3. Computation time of watermarking for different file sizes

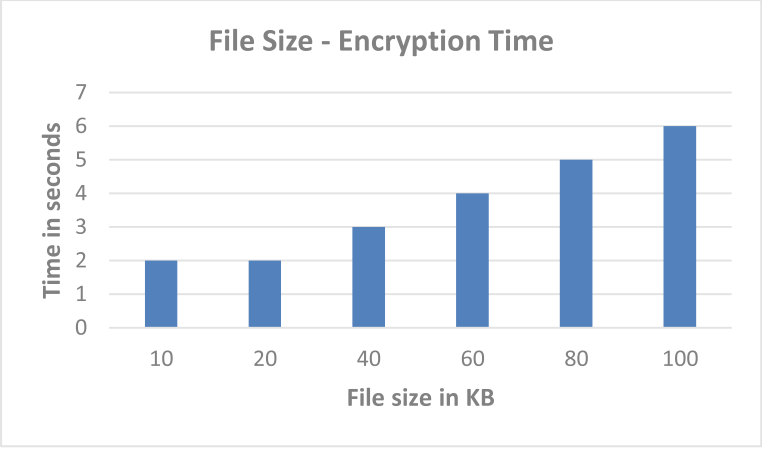

Fig. 4. Computation time of encryption for different file sizes

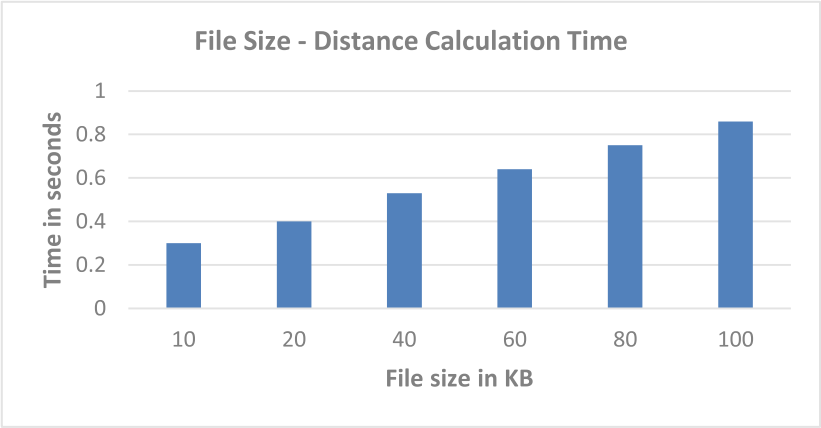

Fig. 5. Computation time to calculate distance for different file sizes

Figure 5 shows the computation time to calculate distance for a particular user at the server side. From Fig. 5 it is evident that with the increasing face image size the time to calculate distance increases linearly.

8 Conclusion

In this paper we propose a secure privacy preserving technique to authenticate a user in a system using user biometrics. We transform the user biometric and watermark the face image with finger print to secure the authentication technique. To preserve the privacy of users watermarked biometric we encrypt it using homomorphic encryption technique. The analysis of our system proves the correctness and privacy of our scheme. The performance analysis shows the efficiency of our technique since the time to authenticate a particular user is less than 11 s where the face image size is 100 KB. For the average face image of less than 10 KB size the proposed technique takes less than 5 s time.

References

1. Riha, Z.: Toward reliable user authentication through biometrics. IEEE Secur. Priv. **1**(3), 45–49 (2003)
2. Katzenbeisser, S.: On the integration of watermarks and cryptography. In: Kalker, T., Cox, I., Ro, Y.M. (eds.) IWDW 2003. LNCS, vol. 2939, pp. 50–60. Springer, Heidelberg (2004)
3. Huang, X., et al.: A generic framework for three-factor authentication: preserving security and privacy in distributed systems. IEEE Trans. Parallel Distrib. Syst. **22**(8), 1390–1397 (2011)

4. Tuyls, P., Akkermans, A.H., Kevenaar, T.A., Schrijen, G.-J., Bazen, A.M., Veldhuis, R.N.: Practical biometric authentication with template protection. In: Kanade, T., Jain, A., Ratha, N.K. (eds.) AVBPA 2005. LNCS, vol. 3546, pp. 436–446. Springer, Heidelberg (2005)
5. Fierrez-Aguilar, J., et al.: Discriminative multimodal biometric authentication based on quality measures. Pattern Recogn. **38**(5), 777–779 (2005)
6. Ahonen, T., Hadid, A., Pietikainen, M.: Face description with local binary patterns: application to face recognition. IEEE Trans. Pattern Anal. Mach. Intell. **28**(12), 2037–2041 (2006)
7. Kumar, A., et al.: Personal verification using palmprint and hand geometry biometric. In: Kittler, J., Nixon, M.S. (eds.) AVBPA 2003. LNCS, vol. 2688, pp. 668–678. Springer, Heidelberg (2003)
8. Jain, A.K., Ross, A., Prabhakar, S.: An introduction to biometric recognition. IEEE Trans. Circuits Syst. Video Technol. **14**(1), 4–20 (2004)
9. Inamdar, V.S., Rege, P.P.: Face features based biometric watermarking of digital image using singular value decomposition for fingerprinting. Int. J. Secur. Appl. **6**(2), 47–60 (2012)
10. Arya, M., Siddavatam, R.: A novel biometric watermaking approach using LWT- SVD. In: Das, V.V., Thomas, G., Lumban Gaol, F. (eds.) AIM 2011. CCIS, vol. 147, pp. 123–131. Springer, Heidelberg (2011)
11. Dogan, S., et al.: A robust color image watermarking with singular value decomposition method. Adv. Eng. Softw. **42**(6), 336–346 (2011)
12. Chang, C.-C., Yih-Shin, H., Tzu-Chuen, L.: A watermarking-based image ownership and tampering authentication scheme. Pattern Recogn. Lett. **27**(5), 439–446 (2006)
13. Mehta, G., Dutta, M.K., Kim, P.S.: An efficient & secure encryption scheme for biometric data using holmes map & singular value decomposition. In: 2014 International Conference on Medical Imaging, m-Health and Emerging Communication Systems (MedCom). IEEE (2014)
14. Rivest, R.L., Shamir, A., Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM **21**(2), 120–126 (1978)
15. Elgamal, T.: A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans. Inform. Theory **31**(4), 469–472 (1985)
16. Paillier, P.: Public-Key Cryptosystems Based on Composite Degree Residuosity Classes. In: Stern, J. (ed.) EUROCRYPT 1999. LNCS, vol. 1592, pp. 223–238. Springer, Heidelberg (1999)
17. Golub, G.H., Reinsch, C.: Singular value decomposition and least squares solutions. Numer. Math. **14**(5), 403–420 (1970)
18. Furon, T., Duhamel, P.: An asymmetric watermarking method. IEEE Trans. Signal Process. **51**(4), 981–995 (2003)
19. Cox, I.J., Doërr, G., Furon, T.: Watermarking is not cryptography. In: Shi, Y.Q., Jeon, B. (eds.) IWDW 2006. LNCS, vol. 4283, pp. 1–15. Springer, Heidelberg (2006)
20. http://www.mathworks.com/matlabcentral/fileexchange/17032-pca-based-face-recognition-system
21. Satish Chandra, D.V.: Digital image watermarking using singular value decomposition. In: The 2002 45th Midwest Symposium on Circuits and Systems, MWSCAS 2002, vol. 3. IEEE (2002)
22. http://math.nist.gov/javanumerics/jama/
23. Lindell, Y., Pinkas, B.: Privacy preserving data mining. In: Bellare, M. (ed.) CRYPTO 2000. LNCS, vol. 1880, pp. 36–54. Springer, Heidelberg (2000)