Multimed Tools Appl
DOI 10.1007/s11042-017-4374-x

Improving biometrics authentication with a multi-factor approach based on optical interference and chaotic maps

Daniel Souza[1] · **Aquiles Burlamaqui**[2] · **Guido Souza Filho**[3]

Received: 5 May 2016 / Revised: 28 October 2016 / Accepted: 9 January 2017

Abstract We propose a method to improve biometric authentication systems using a multifactor approach. For this security scheme a user authenticates successfully using a set of three characteristics related to physical, possession and knowledge factors. Besides biometric authentication representing the physical factor, we propose the use of an optical authentication technique based on two-beam interference and chaotic maps. In this sense, the seed of a chaotic map represents a user password corresponding to a knowledge factor and a resultant interferogram from optical authentication technique is used as a possession factor. The feasibility of our method is tested using numerical simulation. Moreover, key space and statistical analysis are performed to demonstrate the effectiveness of the solution.

Keywords Multi-factor authentication · Biometric authentication · Two-beam interference · Chaotic maps

1 Introduction

Biometrics Authentication is becoming popular and used widely in security information applications. A biometric system uses measurable, unique biological characteristics and

✉ Daniel Souza
danielfaustino@ufersa.edu.br

Aquiles Burlamaqui
aquilesburlamaqui@ect.ufrn.br

Guido Souza Filho
guido@lavid.ufpb.br

[1] Universidade Federal Rural do Semi-Árido - UFERSA, Mossoró, Brazil

[2] Universidade Federal do Rio Grande do Norte - UFRN, Natal, Brazil

[3] Universidade Federal da Paraíba, João Pessoa, Brazil

behaviors to verify human identity. Such characteristics make biometric systems more natural and practical to be used as tools for user authentication. Diversity, revocability, non-invertibility and identification/verification performance are some requirements that biometrics techniques should meet [38]. As a consequence of the increasing use by government and business, such systems became attack target from individuals and criminal organizations. Some attacks target templates are stored in databases. An impostor's copy can replace a biometric template in a database [48]. In addition, an unauthorized user can steal a template and reuse it. In order to circumvent this issues, biometrics protection techniques are proposed in literature. These protection schemes can be categorized into hidden information, biometric cryptosystems, cancelable biometric and hybrid methods [37]. Hidden Information techniques encrypt the biometric template using techniques such as watermarking, steganography, data scrambling and hashcoding, improving secure transmission and storage [28, 29]. Biometric cryptosystems utilize biometric features to generate credentials for cryptography application, replacing password based keys with biometric dependent keys [9, 13, 40, 56]. Cancelable biometric approaches transform the original feature to its protected version with specific functions [24, 40, 69]. The transformation can be invertible or non-invertible and, in either case, the transformation is dependent on a randomly generated user specific key [30]. Hybrid approach combines two or more techniques in order to contour vulnerabilities related to previous approaches. Hybrid methods were developed to fingerprint [47], palmprint [36] and face detection [17].

Other common attacks to biometric systems focus on user interface, presenting a falsified biometric data, e.g. *spoofing* attack [21]. Moreover, there are another way to get access to biometric data. For instance, users can leave fingerprint and palm print marks everywhere they touch and hidden cameras can capture human face and iris. In these cases, even biometric security methods presented above are not completely effective. Therefore, solution that improves biometric systems security are necessary in order to mitigate such issues.

Information processing based on optical techniques have been widely used in security area. The benefits of using such techniques are related to: the intrinsic parallelism of methods, implementation using optical hardware or computer simulation, possibility to work with complex two-dimensional data and large key spaces; that make such techniques a good solution against brute-force attacks. Most works are concentrate on image encryption, data hiding and digital watermarking [43, 57, 62, 64, 65, 67]. Several optical techniques are used for information processing e.g., the double random phase encoding (DRP) developed by Refregier and Javidi [57] and its variations applied in different mathematical transforms domains as Fractional Fourier (FrT) and Fresnel (FrT) [45, 55]. Moreover, techniques that use the Hartley (HT) and Fractional Hartley (HT) transform, gyrator transform and joint transform correlator (JTC) were developed [2, 41, 51]. Furthermore, there are methods based on holography, phase-shifting and two-beam interference [32, 42, 50].

Optical information processing applied to user authentication has also gained attention from researchers last years. Some approaches involve the use of DRP method [4, 66], phase retrieval and truncation [15, 16, 54] and beams interference [3, 22]. Researchers have also investigated how to apply optical processing in conjunction with biometric information for authentication purpose, e.g. [25, 26] proposed optical techniques based on combination of nonlinear JTC method and biometric information for card validation and user authentication. A technique using digital holography was proposed by Kim et al., the authors combine biometrics technology with fully digital holographic storage based on random phase encoded reference beams [31].

There are some issues that can compromise the security of information in optical techniques since they are vulnerable to certain types as known-text and known-cipher attacks [52, 53]. In order to solve this issue, researchers present techniques based on information scrambling before processing the optical technique [34, 63, 72]. Recently, chaotic maps have been used in conjunction with optical methods to provide more consistent information security solutions [8, 11, 14, 71]. Chaotic maps are mathematical functions that exhibit a chaotic behavior and generates different sequence of numbers based on initial conditions. Algorithms based on chaos functions present high sensibility to initial conditions and have been widely used in information security systems, more specifically on scrambling process.

Multi-factor Authentication (MFA) method offers a mechanism that allows the user to get access to a system by providing multiple authentication credentials [5, 39]. These credentials are often based in three groups of information: knowledge, possession and physical presence [18]. Passwords or other combination of information that the user can memorize correspond to knowledge group. Devices, tokens, cards and other physical resources that the user presents to remote access are part of possession group. Finally, physical presence is related to credentials based on biometric information as fingerprint, palm print, iris image, face and voice profile. Although, each group has issues that can compromise a particular factor, a combination of factors makes the system more resistant to attackers since all factors must be compromised. Khan et al. proposed an authentication method using two-factor involving biometrics and passwords [30]. The authors also proposed a hybrid scheme form template security using subspace mapping and arithmetic hashing. Go et al. and Kang et al. proposed two-factor authentication with template security based on password and biometrics (fingerprint information and face recognition, respectively) [20, 27]. Nguyen et al. developed a MFA biometric technique with two factors based on remote authentication using fuzzy commitment and non-invertible transformation [49]. Other two-factor techniques using biometrics were proposed by [6, 23, 33]. Saini and Sinha proposed a set of multi-factor techniques exploring biometrics in combination with log polar transform [59], optics biohashing [60] and DRP method [61]. Yuan et al. developed a multi-factor authentication method using optical encryption and multimodal biometrics where standard biometrics templates are generated real-timely by verification keys, so that storing biometric data is unnecessary [68].

In order to improve security of biometrics systems, a MFA approach is proposed where optical processing and chaotic maps are used in conjunction with biometrics to provide a more sophisticated solution. In this sense, the biometric verification is used as physical presence factor, a phase key generated by optical two-beam interference method represents the possession factor and a password based on chaotic maps is used as knowledge factor. On biometric stage a method based on hybrid shape and orientation description is used to extract features [1]. The configurations of optical method are used as additional secret keys. The proposed method avoids the need to keep the user password and token/smartcard information in system storage.

2 Theoretical description

2.1 Optical interference

An image can be encoded into two phase masks using two-beam interference. Two coherent parallel lights are modulated by two different phase-only masks (M1 and M2) and then

interfere in a half-mirror (HM) in order to generate a complex field distribution on output plane (see Fig. 1). The method proposed by [70] consists in executing the reverse process of interference to separate an image into two phase masks that can be used as keys in a security system. Therefore, considering a non-negative image distribution $O(m, n)$, a complex field distribution can be constructed by

$$O'(m, n) = \sqrt{O(m, n)} \exp(j2\pi\phi(m, n)) \tag{1}$$

where $\phi(m, n)$ is a uniform random distribution between 0 and 1 and j is the imaginary unit. To represent this new complex field as two phase-only masks, $O'(m, n)$ can be expressed as

$$O'(m, n) = \exp(jM1) * h(x, y, l) + \exp(jM2) * h(x, y, l) \tag{2}$$

where $*$ represents the convolution operation, $M1$ and $M2$ are uniform random distributions and $h(x, y, l)$ is the point pulse response function of Fresnel transform defined as follows:

$$h(x, y, l) = \frac{\exp(j2\pi l/\lambda)}{jl\lambda} \exp\left[\frac{j\pi}{l\lambda}(x^2 + y^2)\right] \tag{3}$$

with l as the distance between M1 and M2 to output plane and λ as the wavelength of incident light [70]. Rewriting (2) we obtain

$$\exp(jM1) + \exp(jM2) = D, \tag{4}$$

$$D = \mathcal{F}^{-1}\left\{\frac{\mathcal{F}\{O'(m, n)\}}{\mathcal{F}\{h(x, y, l\}}\right\} \tag{5}$$

where $\mathcal{F}\{\}$ corresponds to Fourier transform and $\mathcal{F}^{-1}\{\}$ corresponds to its inverse. Finally, we can achieve M1 and M2 as follows:

$$M1 = arg(D) - arccos(abs(D)/2) \tag{6}$$

$$M2 = arg(D - \exp(jM1)) \tag{7}$$

where $arg(D)$ returns the phase angle of D and $abs(D)$ returns the complex modulus. For further reading about interference method applied to image encryption please refer to work of Zhang and Wang [70].

2.2 Chebyshev map

A Chebyshev map can be defined as

$$x_{n+1} = f(x_n) = \cos(k \arccos(x_n)) \tag{8}$$

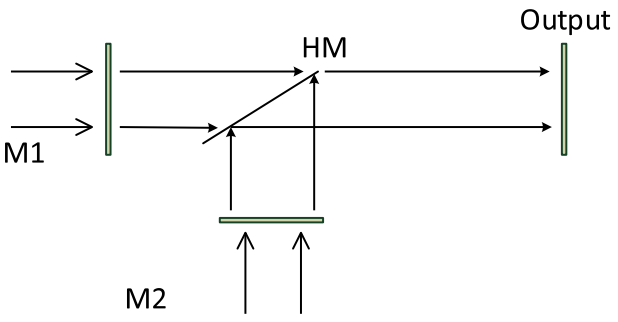


Fig. 1 Two-beams interference method. Phase-only masks M1 and M2 are combined in HM to generate a complex field on output plane

where $-1 \leq x_n \leq 1$ and k is a control parameter. Due to its various statistical properties, Chebyshev maps are an ideal candidates to be used in system for model chaos behavior [19]. For values of $k \in [2, \text{inf}]$, Chebyshev maps produce infinite non periodic chaotic real sequences as illustrated by bifurcation diagram on Fig. 2. Depending on initial value x_0, the chaotic map generates a completely different sequence, so that the initial value can be used as key in a security system. Images can be scrambled using a Chebyshev map, e.g. by shuffling color table index or by changing pixels' values on image using mapping operations such as mod or xor.

3 Proposed technique

In the technique proposed here, the user authenticates in a system by presenting three factors based on characteristics like knowledge, possession and physical presence. As mentioned, the biometrics correspond to physical presence factor. A phase-only mask generated by optical interference described in Section 2.2 is used as the possession factor. The knowledge factor is represented by a numeric password that corresponds to initial value x_0 of a Chebyshev map.

3.1 User registration scheme

The registration process based on the proposed technique is illustrated in Fig. 3. The user needs to generate three keys related to the described factors. First, the user chooses a base image $I_1(m, n)$ from a database or a personal one like the image of his/her face. A support image $I_2(m, n)$ is generated by system with random amplitude distribution. The images $I_1(m, n)$ and $I_2(m, n)$ are encoded into a complex field $C(m, n)$ according to the equation

$$C(m, n) = I_1(m, n) + I_2(m, n) * j \tag{9}$$

The complex field $C(m, n)$ is modulated by a random-phase mask $p(m, n)$ as follow

$$C'(m, n) = C(m, n)p(m, n) \tag{10}$$

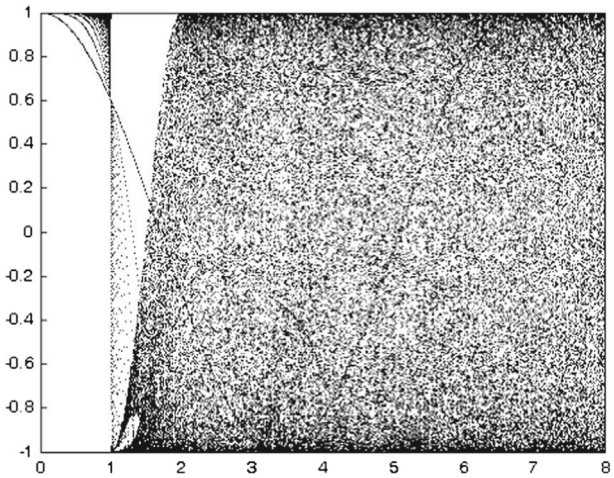


Fig. 2 Bifurcation diagram of Chebyshev map. Nonperiodic chaotic behavior when $k \geq 2$

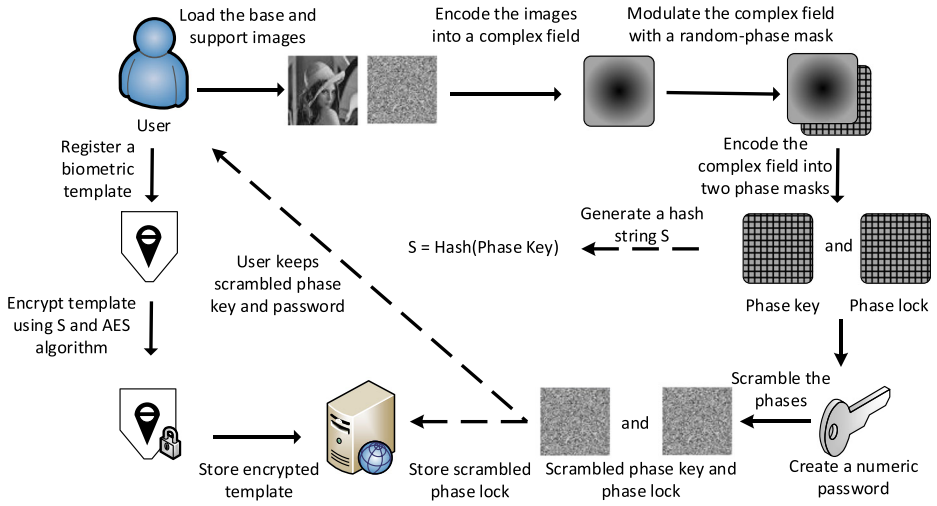


Fig. 3 Registration process in a security system based on the proposed technique

where $C'(m,n)$ is the complex field resultant from modulation and $p(m,n) = exp(j2\pi\phi(m,n))$ with $\phi(m,n)$ as a uniform random distribution between 0 and 1. Thereafter, the complex field $C'(m,n)$ is encoded into two phase-only masks $pl(m,n)$ (phase lock) and $pk(m,n)$ (phase key) as described in (5), (6) and (7). The random-phase mask $p(m,n)$, the wavelength of the illuminating light λ and the distances l between the phase mask and the output plane are only known by the system designer, making the solution more secure against attack attempts.

The second key is a valid biometric characteristic from user like fingerprint, palm print or iris image. For the sake of simplicity, we work with a method to extract biometric template from a fingerprint. The features are extracted from biometric data using a method based on hybrid shape and orientation description [1, 35]. The hybrid descriptor can effectively filter spurious and unnatural minutiae pairings. After feature extraction, the resultant template is encrypted using an AES (Advanced Encryption Standard) algorithm. The key used to encrypt the biometric template is a hash string S resultant from application of a hash function H to the phase key $pk(m,n)$. After feature extraction and encryption, the biometric template is stored.

Finally, the user chooses a numeric password. The phase lock and phase key will be shuffled as follows

$$pl'(m,n) = mod(pl(m,n) + floor(a(m,n) \times 10^{14}), 256) \tag{11}$$

$$pk'(m,n) = mod(pk(m,n) + floor(b(m,n) \times 10^{14}), 256) \tag{12}$$

where $a(m,n)$ and $b(m,n)$ are chaotic sequences generated by a Chebyshev map with x_0 and y_0 as initial value and k_x and k_y as control parameters, respectively. As result, $pl'(m,n)$ and $pk'(m,n)$ correspond to scrambled phase lock and phase key. On mod operation, the parameter value 256 correspond to the pixels levels of a gray scale image with an 8-bit representation. The initial value x_0 corresponds to the password chosen by user. The parameters k_x, k_y and y_0 are another security information only known by system designer. The phase lock $pl'(m,n)$ is stored in the authentication system and the user keeps the phase key $pk'(m,n)$ stored as an interferogram in a security device, e.g. a card or token.

In this method two images are used in the interference process to improve the security requirements. The addition of a support image allows the use of a second chaotic map increasing the number of secret keys. Moreover, the random-phase mask $p(m, n)$ cannot be used as a secret key in the authentication process if we use only one image in two-beam interference process, since the base image can be recovered without knowing the random-phase mask. The random-phase mask is necessary to recover correctly the original base image in the authentication process when two images and encoding, both into a complex field are used, so that $p(m, n)$ is another secret key. The key used to encrypt the biometric template is generated before the process of phase key scrambling with the chaotic sequence to avoid the possibility that an unauthorized user accesses the physical device and decrypt the biometric template.

3.2 Authentication process

The authentication process occurs in three steps as shown in Fig. 4. In the first step the user inserts the security card or token where the phase key is recorded and inputs the numeric password. As described in Section 3.1, the password is used as initial value x_0 in conjunction with system information (y_0, k_x and k_y) to generate the correct chaotic sequences $a(m, n)$ and $b(m, n)$ necessary to decode the scrambled phases. Then, the original phases $pl(m, n)$ and $pk(m, n)$ are recovered as

$$pl(m, n) = mod(pl'(m, n) - floor(a(m, n) \times 10^{14}), 256) \tag{13}$$

$$pk(m, n) = mod(pk'(m, n) - floor(b(m, n) \times 10^{14}), 256) \tag{14}$$

In the second step, the system collects the biometric information from user and extracts the corresponding features generating the template that will be used to validate the user identity. The hash string S is reconstructed by applying the hash function H to the reconstructed phase key $pk(m, n)$. The reconstructed phase key $pk(m, n)$ is used instead of the scrambled phase key $pk'(m, n)$ to improve template security so that two factors are necessary to decrypt the biometric data. The hash string S is used as input key to the AES algorithm in order to decrypt the biometric template stored. Finally, the captured template is compared with the stored template. If the information matches based on a score function and a pre-configured threshold, the system loads the additional information required to proceed with authentication process.

In the third step, with the unscrambled phase key and phase lock, it is possible to reconstruct the complex field $C'(m, n)$ using (2). Then, the original base image can be obtained as

$$I_1(m, n) = Re\{C'(m, n)p^*(m, n)\} \tag{15}$$

where $p^*(m, n)$ is the complex conjugate of the random-phase mask $p(m, n)$ and the operations $Re\{\}$ represents the real part of a complex number. In order to finalize the authentication process the decoded base image is compared to the original base image. If the comparison value is over a defined threshold, the user gains access to the system, otherwise the authentication process fails. In this work, the authors chose the MSE (Mean Square Error) metric to evaluate the similarity between the original base image and the reconstructed base image.

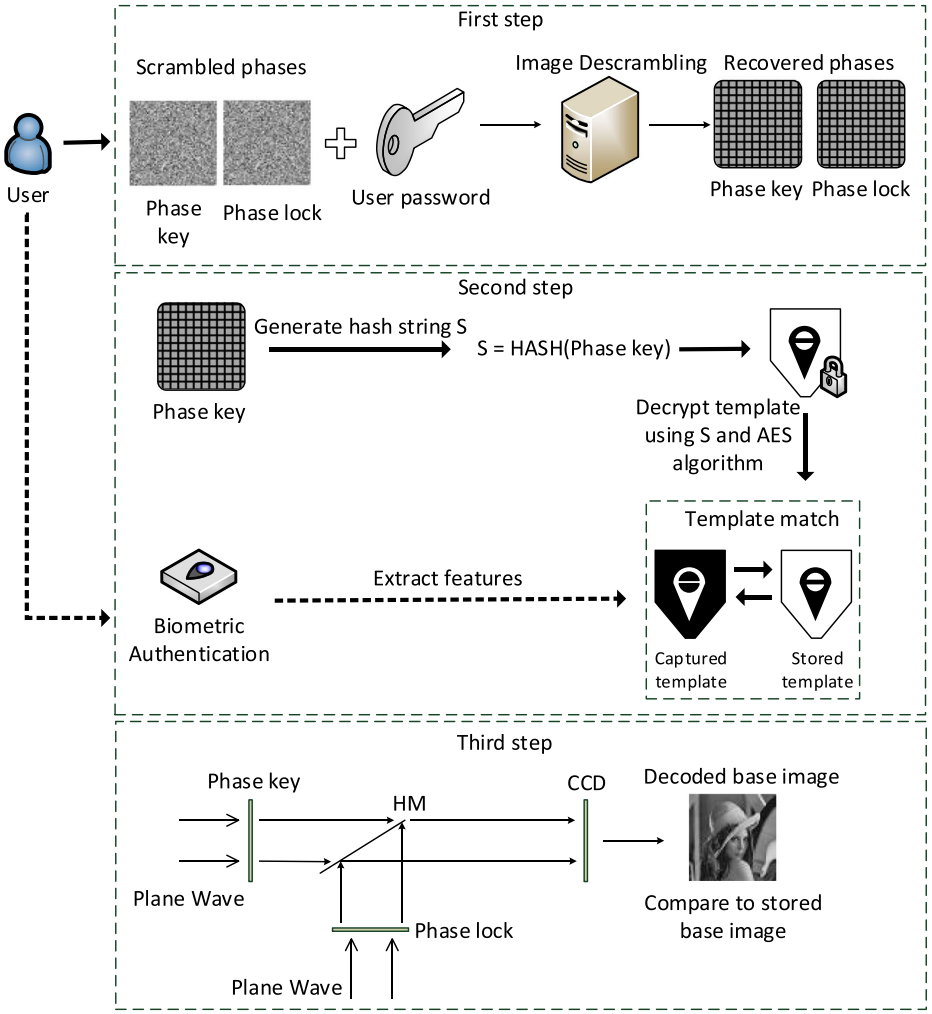


Fig. 4 Multi-factor authentication process. First the biometric authentication is performed, the scrambled phases are decoded in second step and the original base image is obtained in third step using interference method

4 Numerical simulation

Our simulations focus on analysis of phase key and user password since these factors play a role key on security of entire method and, particularly, on biometric template security. The biometric template security is widely discussed on reference presented in Section 1. Also, AES standard principles and security analysis are extensively discussed in literature [7, 12, 46]. Numerical simulations and analysis are performed using the software Matlab.

The image of Lena with 256 x 256 pixels and 256 grey levels is used as base image for registration and authentication process. In the interference process the configuration values are chosen according to [70] with an image size of 5 cm x 5 cm, wavelength of illuminating light $\lambda = 633nm$ and distance between the phase masks and input plane l = 20 cm. The random-phase mask $p(m, n)$ has its values randomly distributed over the interval $[0, 2\pi]$. The numeric password must be between 6 and 14 digits. This numeric password represents the initial value x_0 of the chaotic sequence $a(m, n)$ used to shuffle the phase key. In order to simulate the image scrambling using (8), (11) and (12), the values chosen were $x_0 = 0.18642564$, $y_0 = 0.30860348$, $k_x = 4.55214475$ and $k_y = 5.24933281$.

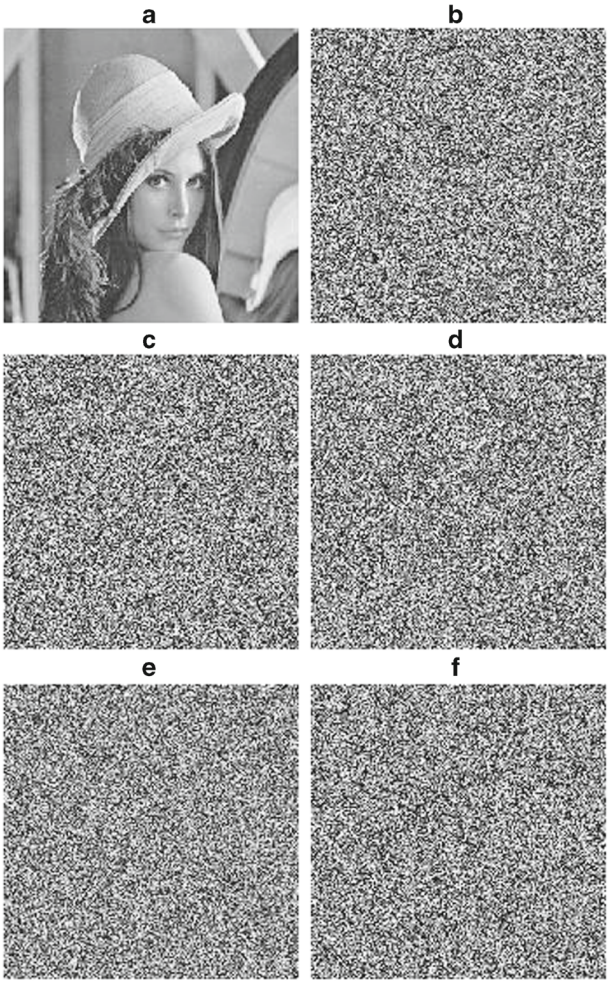


Fig. 5 Encoding base image and generating phase masks. **a** Base image. **b** Support image. **c** Phase lock. **d** Phase key. **e** Scrambled phase key with $x_0 = 0.18642564$ (user password) and $k_x = 4.55214475$. **d** Scrambled phase lock with $y_0 = 0.30860348$ and $k_y = 5.24933281$

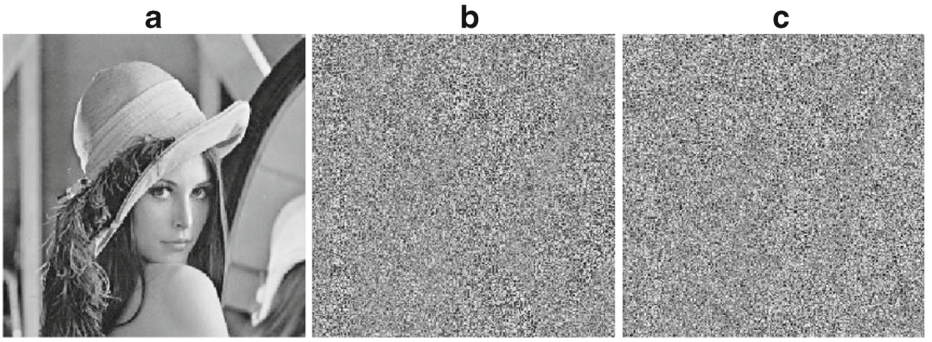


Fig. 6 Decoding base image with correct/incorrect keys. **a** Base image decoded with correct keys. **b** Base image decoded with incorrect random-phase mask. **c** Base image decoded with incorrect password

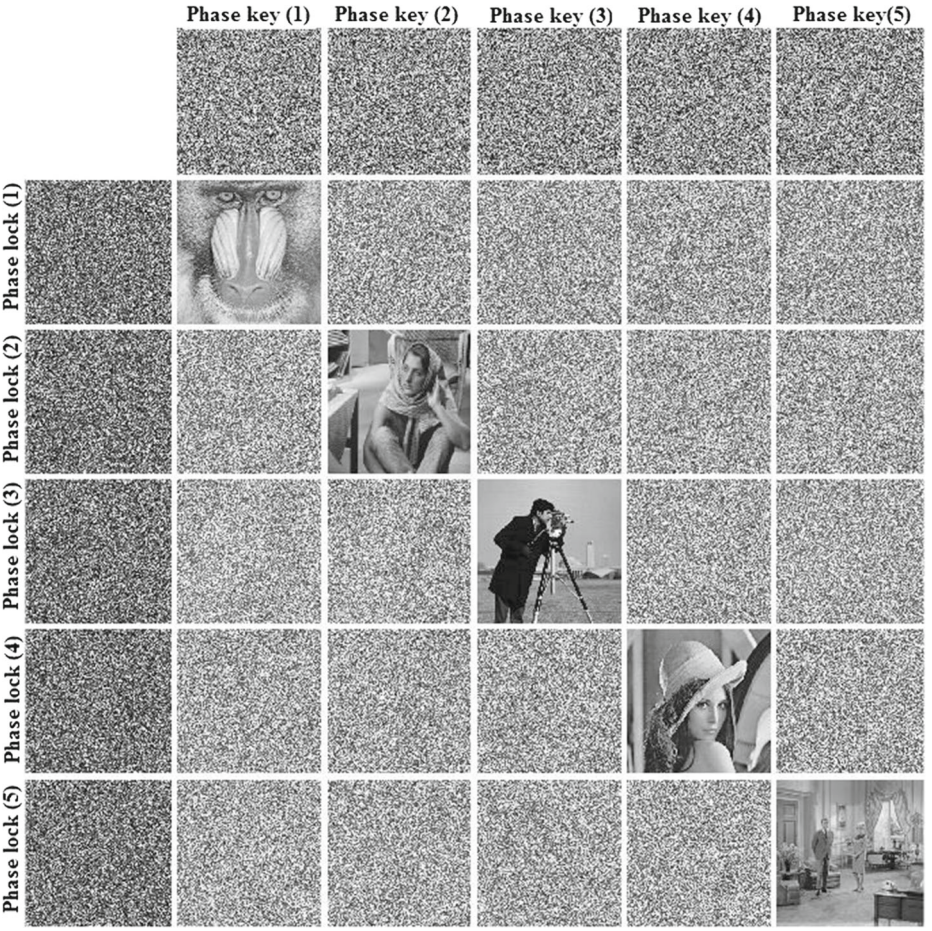


Fig. 7 Different authentication scenarios as a various phase masks combination

Table 1 MSE Values for output images after reconstruction with various phase data combination as showed in Fig. 7

	Phase Key 1	Phase Key 2	Phase Key 3	Phase Key 4	Phase Key 5
Phase Lock 1	$1.0847e^{-25}$	0.0982	0.0971	0.0995	0.0988
Phase Lock 2	0.1338	$1.1662e^{-25}$	0.1331	0.1335	0.1326
Phase Lock 3	0.1541	0.1539	$9.3164e^{-26}$	0.1531	0.1527
Phase Lock 4	0.1344	0.1330	0.1319	$1.6304e^{-25}$	0.1322
Phase Lock 5	0.1089	0.1072	0.1072	0.1072	$1.4415e^{-25}$

Figure 5 shows the experiments results after interference process and phase scrambling. The Fig. 5a and b show the base and support images used in registration. Figure 5c and d show the phase lock and phase key obtained through interference method. The user password represented by x_0 and the other system settings y_0, k_x and k_y were used to generate the scrambled phases as shown in Fig. 5e and f.

In the authentication process, the decoding and validation of base image will happen. The user will insert the security card and input the numeric password in order to validate his identity. Figure 6 shows the different results of decoding the base image using correct/incorrect keys. The Fig. 6a shows the base image decoded using the correct keys. Figure 6b and c show results of decoding the base image using a wrong random-phase mask and a incorrect password, respectively.

In order to finalize the authentication process the resultant image must be compared to original image using MSE. A threshold value of 10^{-20} was used as limit to validate the user authentication. Figure 7 shows the reconstruction of some base images using different phase keys and their corresponding phase locks. In Tables 1 and 2 different scenarios of authentication and the value of MSE are shown after comparing reconstructed images and their corresponding base image with various combinations of phase masks and initial value of x_0. In Tables 1 and 2, the values of MSE in diagonal, correspond to images reconstructed with correct phase keys and user passwords, respectively. The other values correspond to images reconstructed with wrong keys and consequently the authentication process fails since the MSE values are above the threshold.

The dependence of authentication process on correct configuration of system parameters are shown in Figs. 8 and 9. The chaotic map used to scramble the phase key and phase lock masks are very sensitive to variations on initial value and control parameters, so that only when y_0, k_x and k_y are exactly the correct ones, the MSE reaches small values necessary to validate the authentication process. Similarly, the wavelength λ and distance between masks and output plane l are sensitive to small changes as showed in Fig. 9. Therefore, in

Table 2 Output image MSE after reconstruction using different values of x_0

	$x_0 = 0.18642564$	$x_0 = 0.50702672$	$x_0 = 0.66637284$	$x_0 = 0.96872668$	$x_0 = 0.47044470$
Madril	$2.7559e^{-25}$	0.0970	0.0986	0.1006	0.0974
Barbara	0.1341	$1.6245e^{-25}$	0.1324	0.1327	0.1324
Cameraman	0.1559	0.1544	$1.6764e^{-25}$	0.1522	0.1524
Lena	0.1330	0.1335	0.1305	$1.2923e^{-25}$	0.1330
Living Room	0.1095	0.1113	0.1124	0.1082	$1.0416e^{-25}$

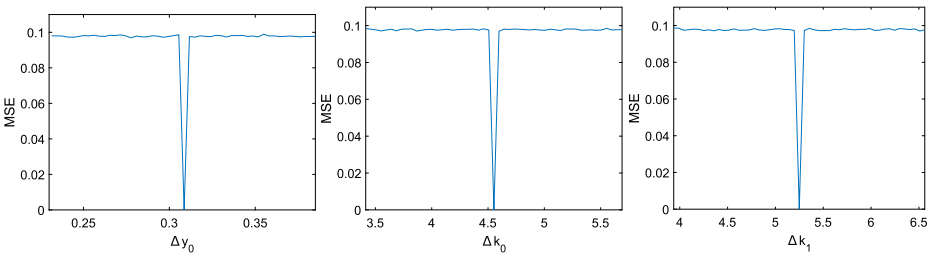


Fig. 8 MSE behavior on changing Δy_0, Δk_x and Δk_y

case of small deviations, the MSE increases quickly and the authentication process fails. These properties make the system more resilient to attacks in which the individuals try to reproduce system features.

5 Key space analysis

In this method three steps are used in authentication process. The firt step consists of a password with up to 14 digits that is used as seed of a chaotic sequence. Each digit of this password can assume 10 values (0-9), which results in 10^{14} combinations. Beside this, the total number of key combination for a Chebyshev map is approximately $4\pi \times 10^{30}$ [10]. In second step, the force of possession factor is related to resolution of the phase key so that, based on an 8-bit representation, a $n \times n$ interferogram has $256^{n \times n}$ possibilities. Considering the resolution used in this paper, a space of $256^{256 \times 256}$ combinations must be tested in order to discover the correct phase key. Since the optical and chaotic decoding are significantly sensitive to the input values, the key space is large enough to be resilient against brute force attacks. The biometric information cannot be recovered by brute-force attacks. The biometric template is securely stored and cannot be recovered without the user password and scrambled phase key.

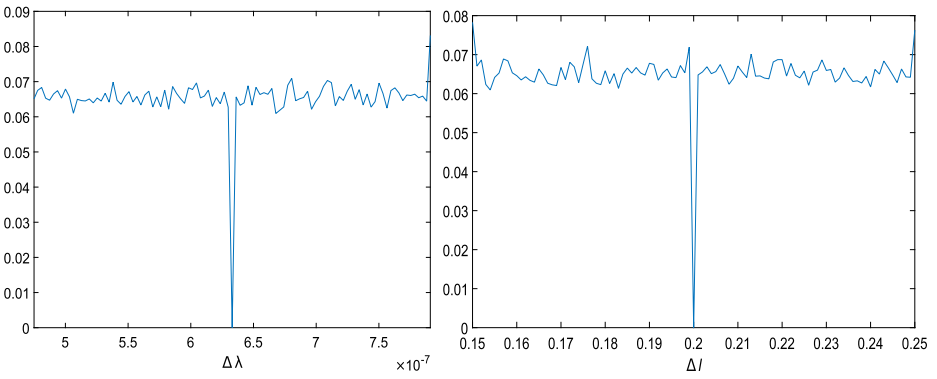


Fig. 9 MSE behavior of on changing $\Delta\lambda$ and Δl

Table 3 Correlation coefficients for various base images and their corresponding phase keys

Direction	Horizontal	Vertical	Main Diagonal	Anti-Diagonal
Barbara	0.856160	0.882802	0.794241	0.883678
Phase Key for Barbara	0.047055	0.028869	0.038788	0.047026
Lena	0.954747	0.986076	0.881300	0.917006
Phase Key for Lena	009810	−0.003845	0.076336	−0.023175
Living Room	0.929607	0.692492	0.868747	0.895583
Phase Key for Living Room	−0.084112	0.036197	0.031814	−0.016817

6 Statistical analysis

6.1 Correlation coefficient

The proposed method uses a resultant interferogram from combination of a base and a support image as one of authentications keys. In this case, a strong key should have a weak correlation between adjacent values in the resultant interferogram. The (16) was used to calculate de correlation coefficient [44]. A sample of 500 pair of adjacent values from base images and correspondent phase keys were used. The correlation was calculated in horizontal, vertical, main diagonal and anti-diagonal directions. Table 3 shows the results for three base images and the correspondents phase keys generated in registration process. The base images have high correlation between adjacent values, however the resultants phase keys are weakly correlated. Figure 10a–h shows the adjacent values correlation results for base

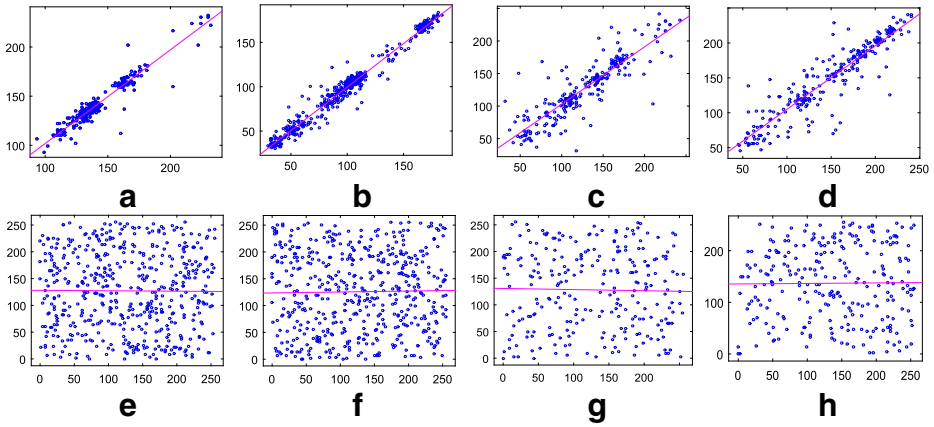


Fig. 10 Correlation results for Lena's base image and its corresponding phase key: **a** Lena's image horizontal correlation; **b** Lena's image Vertical correlation; **c** Lena's image main diagonal correlation; **d** Lena's image Anti-diagonal correlation; **e** Phase key horizontal correlation of; **f** Phase key vertical correlation; **g** Phase key main diagonal correlation; **h** Phase key anti-diagonal correlation

image Lena and its correspondent phase key. The results indicate that the proposed scheme can produce good phase keys to be used as possession factor in authentication process.

$$
\begin{aligned}
r_{xy} &= \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}, \\
cov(x,y) &= \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)), \\
D(x) &= \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2, E(x) = \sum_{i=1}^{N}(x_i)
\end{aligned}
\tag{16}
$$

6.2 Histogram

The histogram of an image carries important information about pixels distribution and statistical characteristics. An ideal phase key should have a uniform and different histogram compared to its base image. The histogram analysis was performed to three base images Mandrill, Cameraman and Barbara. Figure 11 shows the three base images histogram distributions and their correspondent phase keys. Each base image has a specific distribution. After registration process each phase key generated has a histogram pattern close to a uniform distribution. This characteristic indicates that the phase keys are resilient against statistical attacks.

6.3 Information entropy

The information entropy is used to measure randomness of values distribution on phase key after optical and chaotic encoding. The entropy of the phase keys is calculated using (17) [58]. The ideal entropy value for the resultant phase keys should be 8, indicating a high level of randomness. Table 4 shows the entropy for five phase keys generated from their respective

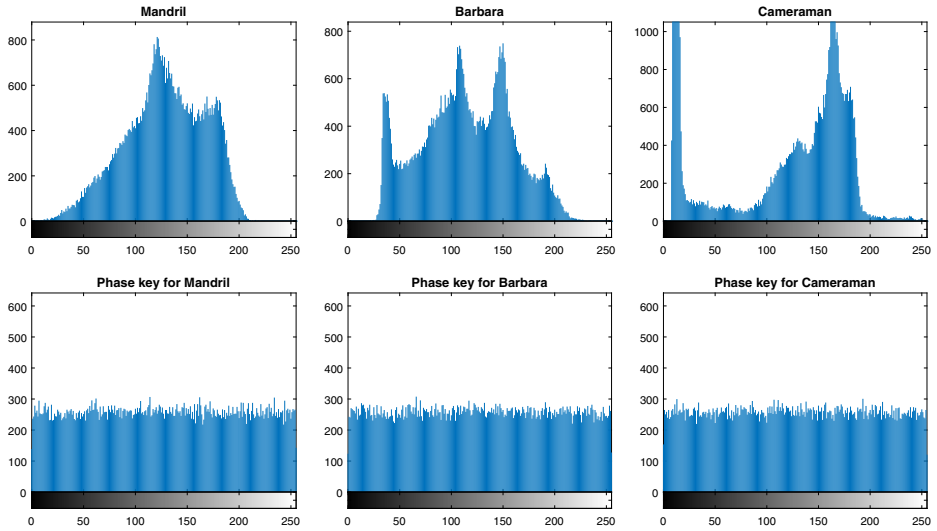


Fig. 11 Histogram for base image and corresponding phase keys

Table 4 Entropy values for phase keys constructed from their respective base images

	Entropy
Phase key for Mandril	7.995777
Phase key for Barbara	7.995331
Phase key for Cameraman	7.995500
Phase key for Lena	7.995116
Phase key for Living Room	7.996087

base images. The obtained values are close to 8 indicating a high level of randomness and a good performance in avoiding entropy attacks.

$$H(S) = \sum_{i=1}^{N} P(s_i) \log_2 \frac{1}{P(s_i)} \tag{17}$$

7 Comparison with other similar methods

In Section 1 we discussed a set of multi-factor authentication methods. As mentioned, optical technique was also applied to development of user authentication in conjunction with biometrics. Table 5 shows a comparison between some techniques presented in this work and our proposed scheme. Basically, most techniques use a multi-factor approach based on two factor as credentials with biometrics and password. The use of three factors offers a most resilient authentication technique adding a level of security to the process. Every method that stores templates in system database offer a kind of security to this data. In techniques proposed by Khan et al. [30] and Go et al. [20] the template security mechanism depends exclusively on user password. Kang et al. [27] designed a method where template security depends on user password and some systems parameters as random salt and isolation matrix. Saine et al. [61] and Yuan et al. [68] don't store template in system database. They use optical techniques based on interferometry and DRP method to generate phase masks from biometric templates and validate user in real time. The method proposed by Yuan et al. [68] use three factors all based on biometric data so that their technique is weak against all attacks that involve biometric theft or copy. Analogously, Saine et al. [61] designed a method where just one biometric factor is required and no other factor is used implying in the same biometric theft or copy problems. Additional parameters configured at system level can improve method security avoiding illegal user from reproducing

Table 5 Comparison between multi-factor authentication methods

Method	Factors	Template Security	Non biometric factors	System keys
Khan et al. [30]	2	Random projection and hashing	Password	none
Go et al. [20]	2	Split and rearrange template	Password	none
Kang et al. [27]	2	Matrix permutation	Password	yes
Yuan et. al. [68]	3	Not stored	None	yes
Saine et al. [61]	1	Not stored	None	yes
Proposed method	3	Hash function and AES encryption	Password and token	yes

the authentication infrastructure. These additional parameters are extra keys only known by system designer. The proposed method has three factors improving system diversity in relation to authentication credentials. Regarding template security, our method uses an AES algorithm to encrypt biometric data. This encryption process depends on user password and phase key. Also, the additional parameters as random phase mask, wavelength, distance from mirrors and control parameters from chaotic maps are necessary to correctly decrypt the biometric template.

8 Conclusion

In this paper, we proposed a new technique that improves biometric authentication using a multi-factor approach where: biometric characteristic corresponds to physical factor, and optical encryption and chaotic maps are used to represent respectively possession and knowledge factors. In the proposed scheme a user registers in a system firstly recording a biometric template. The user chooses a base image that will be encoded using two-beam interference generating a phase key. This phase key is used to encrypt biometric data using a hash function and AES algorithm. Then, the user chooses a password (knowledge factor) that will be used as a seed to a chaotic sequence based on a Chebyshev map. The chaotic sequence is used to scramble the phase key, resulting in the possession factor. The user keeps a phase key stored as an interferogram in a smartcard/token and the password.

The user's authentication depends on presentation of the three factors. The biometric template is securely stored in the system and depends on user's password and smartcard/token to be decrypted. Also, a set of parameters configured on the system are necessary to decrypt biometric data and give user access to the system. These additional parameters are extra keys only known by system designer. This characteristic improves system security against attacks where t illegal user tries to reproduce the authentication system.

The simulation results and analyses show the robustness of the proposed method with a high sensitivity to initial values, resistance against brute-force and other common attacks, large key space and good statistical properties. The proposed scheme can be used in applications that require a high level of security as systems used by banks, government and businesses. As future work, the authors are working on improving the proposed method to avoid the need of template information storage on system database based on the idea presented in [68]. Other future work would be related to improving the system to allow user credentials to be updated securely.

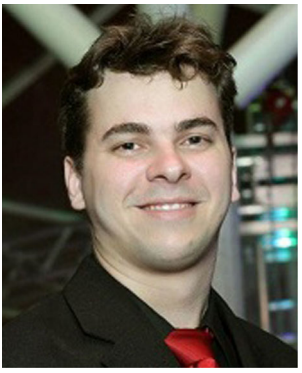
References

1. Abraham J, Gao J, Kwan P (2011) Fingerprint matching using a hybrid shape and orientation descriptor. INTECH Open Access Publisher
2. Abuturab MR (2013) Color image security system based on discrete hartley transform in gyrator transform domain. Opt Lasers Eng 51(3):317–324
3. Abuturab MR (2013) Information authentication system using interference of two beams in gyrator transform domain. Appl Opt 52(21):5133–5142
4. Alfalou A, Mansour A (2009) Double random phase encryption scheme to multiplex and simultaneous encode multiple images. Appl Opt 48(31):5933–5947

5. Amin R, Islam SH, Biswas G, Khan MK, Leng L, Kumar N (2016) Design of an anonymity-preserving three-factor authenticated key exchange protocol for wireless sensor networks. Comput Netw 101:42–62
6. Anzaku ET, Sohn H, Ro YM (2010) Multi-factor authentication using fingerprints and user-specific random projection. In: APWeb, pp 415–418
7. Blömer J, Seifert JP (2003) Fault based cryptanalysis of the advanced encryption standard (AES). Springer, Berlin Heidelberg, pp 162–181
8. Borujeni SE, Eshghi M (2013) Chaotic image encryption system using phase-magnitude transformation and pixel substitution. Telecommun Syst 52(2):525–537
9. Cavoukian A, Stoianov A et al (2009) Biometric encryption chapter from the encyclopedia of biometrics. Office of the Information and Privacy Commissioner
10. Chen Jx, Zhu Zl, Liu Z, Fu C, Zhang Lb, Yu H (2014) A novel double-image encryption scheme based on cross-image pixel scrambling in gyrator domains. Opt Express 22(6):7349–7361
11. Chen Jx, Zhu Zl, Fu C, Zhang Lb, Yu H (2015) Analysis and improvement of a double-image encryption scheme using pixel scrambling technique in gyrator domains. Opt Lasers Eng 66:1–9
12. Daemen J, Rijmen V (2013) The design of Rijndael: AES-the advanced encryption standard. Springer Science & Business Media
13. Dodis Y, Ostrovsky R, Reyzin L, Smith A (2008) Fuzzy extractors: how to generate strong keys from biometrics and other noisy data. SIAM J Comput 38(1):97–139
14. Elshamy AM, Rashed AN, Mohamed AENA, Faragalla OS, Mu Y, Alshebeili SA, Abd El-Samie F (2013) Optical image encryption based on chaotic baker map and double random phase encoding. J Lightwave Technol 31(15):2533–2539
15. Fan D, Meng X, Wang Y, Yang X, Peng X, He W, Dong G, Chen H (2013) Optical identity authentication scheme based on elliptic curve digital signature algorithm and phase retrieval algorithm. Appl Opt 52(23):5645–5652
16. Fan D, Meng X, Wang Y, Yang X, Pan X, Peng X, He W, Dong G, Chen H (2015) Multiple-image authentication with a cascaded multilevel architecture based on amplitude field random sampling and phase information multiplexing. Appl Opt 54(11):3204–3215
17. Feng YC, Yuen PC, Jain AK (2010) A hybrid approach for generating secure and discriminating face template. IEEE Trans Inf Forens Secur 5(1):103–117
18. Fleischhacker N, Manulis M, Azodi A (2014) A modular framework for multi-factor authentication and key exchange. In: Security standardisation research. Springer, pp 190–214
19. Geisel T, Fairen V (1984) Statistical properties of chaos in chebyshev maps. Phys Lett A 105(6):263–266
20. Go W, Lee K, Kwak J (2014) Construction of a secure two-factor user authentication system using fingerprint information and password. J Intell Manuf 25(2):217–230
21. Haupt G, Mozer T (2015) Assessing biometric authentication: a holistic approach to accuracy. Biom Technol Today 2015(3):5–8
22. He W, Peng X, Meng X, Liu X (2012) Optical hierarchical authentication based on interference and hash function. Appl Opt 51(32):7750–7757
23. Huang X, Xiang Y, Chonka A, Zhou J, Deng RH (2011) A generic framework for three-factor authentication: preserving security and privacy in distributed systems. IEEE Trans Parallel Distrib Syst 22(8): 1390–1397
24. Jassim S, Al-Assam H, Sellahewa H (2009) Improving performance and security of biometrics using efficient and stable random projection techniques. In: Proceedings of 6th international symposium on image and signal processing and analysis, 2009. ISPA 2009. IEEE, pp 556–561
25. Javidi B, Sergent A (1997) Fully phase encoded key and biometrics for security verification. Optical Eng 36(3):935–942
26. Javidi B, Ahouzi E (1998) Optical security system with fourier plane encoding. Appl Opt 37(26):6247–6255
27. Kang J, Nyang D, Lee K (2014) Two-factor face authentication using matrix permutation transformation and a user password. Inform Sci 269:1–20
28. Khan MK, Zhang J (2008) Multimodal face and fingerprint biometrics authentication on space-limited tokens. Neurocomputing 71(13):3026–3031
29. Khan MK, Zhang J, Tian L (2007) Chaotic secure content-based hidden transmission of biometric templates. Chaos Solitons Fract 32(5):1749–1759
30. Khan SH, Akbar MA, Shahzad F, Farooq M, Khan Z (2015) Secure biometric template generation for multi-factor authentication. Pattern Recog 48(2):458–472

31. Kim J, Choi J, An J, Kim N, Lee K (2005) Digital holographic security system based on random phase encoded reference beams and fingerprint identification. Opt Commun 247(4):265–274
32. Kong D, Shen X, Shen Y, Wang X (2014) Multi-image encryption based on interference of computer generated hologram. Optik-Int J Light Electron Opt 125(10):2365–2368
33. Kumar A, Lee HJ (2013) Multi-factor authentication process using more than one token with watermark security. In: Future information communication technology and applications. Springer, pp 579–587
34. Kumar P, Joseph J, Singh K (2011) Optical image encryption using a jigsaw transform for silhouette removal in interference-based methods and decryption with a single spatial light modulator. Appl Opt 50(13):1805–1811
35. Kwan PW, Gao J, Guo Y (2006) Fingerprint matching using enhanced shape context. In: Proceedings of the image and vision computing New Zealand. Citeseer, pp 115–120
36. Leng L, Zhang J (2011) Dual-key-binding cancelable palmprint cryptosystem for palmprint protection and information security. J Netw Comput Appl 34(6):1979–1989
37. Leng L, Zhang J (2011) Dual-key-binding cancelable palmprint cryptosystem for palmprint protection and information security. J Netw Comput Appl 34(6):1979–1989. Control and Optimization over Wireless Networks
38. Leng L, Zhang J (2013) Palmhash code vs. palmphasor code. Neurocomputing 108:1–12
39. Leng L, Teoh ABJ, Li M, Khan MK (2014) A remote cancelable palmprint authentication protocol based on multi-directional two-dimensional palmphasor-fusion. Secur Commun Netw 7(11): 1860–1871
40. Li H, Zhang J, Zhang Z (2010) Generating cancelable palmprint templates via coupled nonlinear dynamic filters and multiple orientation palmcodes. Inform Sci 180(20):3876–3893
41. Li J, Zheng T, Liu Qz, Li R (2012) Double-image encryption on joint transform correlator using two-step-only quadrature phase-shifting digital holography. Opt Commun 285(7):1704–1709
42. Li J, Zheng T, Liu Qz, Li R (2012) Image encryption with two-step-only quadrature phase-shifting digital holography. Optik-Int J Light Electron Opt 123(18):1605–1608
43. Li J, Li J, Pan Y, Li R (2014) Optical image hiding with a modified mach–zehnder interferometer. Opt Lasers Eng 55:258–261
44. Liu H, Wang X (2010) Color image encryption based on one-time keys and robust chaotic maps. Comput Math Appl 59(10):3320–3327
45. Liu Z, Li S, Liu W, Wang Y, Liu S (2013) Image encryption algorithm by using fractional fourier transform and pixel scrambling operation based on double random phase encoding. Opt Lasers Eng 51(1):8–14
46. Miller FP, Vandome AF, McBrewster J (2009) Advanced encryption standard. Alpha Press
47. Nagar A, Nandakumar K, Jain AK (2010) A hybrid biometric cryptosystem for securing fingerprint minutiae templates. Pattern Recog Lett 31(8):733–741
48. Nandakumar K (2008) Multibiometric systems: fusion strategies and template security. ProQuest
49. Nguyen TAT, Nguyen DT, Dang TK (2015) A multi-factor biometric based remote authentication using fuzzy commitment and non-invertible transformation. In: Information and communication technology-EurAsia conference. Springer, pp 77–88
50. Niu CH, Wang XL, Mao XH (2012) Multiple-image hiding based on interference principle. Opt Quant Electron 43(6–10):91–99
51. Nomura T, Javidi B (2000) Optical encryption using a joint transform correlator architecture. Opt Eng 39(8):2031–2035
52. Peng X, Zhang P, Wei H, Yu B (2006) Known-plaintext attack on optical encryption based on double random phase keys. Opt Lett 31(8):1044–1046
53. Rajput SK, Nishchal NK (2013) Known-plaintext attack-based optical cryptosystem using phase-truncated fresnel transform. Appl Opt 52(4):871–878
54. Rajput SK, Nishchal NK (2014) An optical encryption and authentication scheme using asymmetric keys. JOSA A 31(6):1233–1238
55. Rajput SK, Nishchal NK (2014) Fresnel domain nonlinear optical image encryption scheme based on gerchberg–saxton phase-retrieval algorithm. Appl Opt 53(3):418–425
56. Rathgeb C, Uhl A (2011) A survey on biometric cryptosystems and cancelable biometrics. EURASIP J Inf Secur 2011(1):1
57. Refregier P, Javidi B (1995) Optical image encryption based on input plane and fourier plane random encoding. Opt Lett 20(7):767–769

58. Rhouma R, Meherzi S, Belghith S (2009) Ocml-based colour image encryption. Chaos Solitons Fractals 40(1):309–318
59. Saini N, Sinha A (2010) Optics based biometric encryption using log polar transform. Opt Commun 283(1):34–43
60. Saini N, Sinha A (2011) Soft biometrics in conjunction with optics based biohashing. Opt Commun 284(3):756–763
61. Saini N, Sinha A (2013) Biometrics based key management of double random phase encoding scheme using error control codes. Opt Lasers Eng 51(8):1014–1022
62. Situ G, Zhang J (2004) A lensless optical security system based on computer-generated phase only masks. Opt Commun 232(1):115–122
63. Sui L, Gao B (2013) Color image encryption based on gyrator transform and arnold transform. Opt Laser Technol 48:530–538
64. Wang H (2012) A no interference method for image encryption and decryption by an optical system of a fractional fourier transformation and a fourier transformation. In: Advances in multimedia, software engineering and computing, vol 1. Springer, pp 671–676
65. Wang X, Chen W, Chen X (2014) Optical binary image encryption using aperture-key and dual wavelengths. Opt Express 22(23):28,077–28,085
66. Wang X, Chen W, Chen X (2015) Optical information authentication using compressed double-random-phase-encoded images and quick-response codes. Opt Express 23(5):6239–6253
67. Yang YG, Xia J, Jia X, Zhang H (2013) Novel image encryption/decryption based on quantum fourier transform and double phase encoding. Quant Inf Process 12(11):3477–3493
68. Yuan S, Zhang T, Zhou X, Liu X, Liu M (2013) An optical authentication system based on encryption technique and multimodal biometrics. Opt Laser Technol 54:120–127
69. Zhang J, Khan MK (2011) Cancelable palmcode generated from randomized gabor filters for palmprint template protection
70. Zhang Y, Wang B (2008) Optical image encryption based on interference. Opt Lett 33(21):2443–2445
71. Zhang Y, Xiao D (2013) Double optical image encryption using discrete chirikov standard map and chaos-based fractional random transform. Opt Lasers Eng 51(4):472–480
72. Zhou NR, Hua TX, Gong LH, Pei DJ, Liao QH (2015) Quantum image encryption based on generalized arnold transform and double random-phase encoding. Quant Inf Process 14(4):1193–1213



Daniel Souza received the Ms. degree from Federal University of Paraíba, Brazil, in 2010. He is an assistent professor at Federal University of Semi-Arido, Brazil and PhD student at Federal University of Rio Grande do Norte. His research interests include Digital Television, Virtual Reality, Multimedia Applications and Multimedia Security.

Aquiles Burlamaqui is an associete professor at Federal University of Rio Grande do Norte, Brazil. His research interests include Virtual Environment, Robotics, Software Engineering and Multimedia Applications. Burlamaqui has a PhD in Eletrical Engineering from Federal University of Rio Grande do Norte, Brazil.

Guido Souza Filho is an associate professor and the coordinator of the Laboratory for Applications of Digital Video (LAVID) at the Federal University of Paraíba, Brazil. His research interests include dependability in multimedia systems, hypermedia, Digital TV, distributed systems, distributed multimedia applications, and computer networks and video. Souza Filho has a PhD in computer science from Catholic University of Rio de Janeiro, Brazil.