Digital holographic security system based on multiple biometrics

ALOKA SINHA AND NIRMALA SAINI
Department of Physics,
Indian Institute of Technology Delhi
Indian Institute of Technology Delhi, Hauz Khas, New Delhi -110 016
India
aloka@physics.iitd.ernet.in

Abstract: A new multiple biometrics based encryption technique using digital holographic security system has been proposed. In this method, a face image of an enrolled person can be spatially multiplexed by a phase mask. This phase mask has been generated by the fingerprint of the enrolled person. In order to overcome the problem of rotation and scaling of the fingerprint, the log polar transform of the fingerprint has been used. In the previous techniques based on the double random phase encoding two random phase masks have been used. In our technique, along with one random phase mask, the phase mask generated by the fingerprint has been used instead of the second random phase mask. This method has advantage over other digital holographic security system due to its capability of authentication by using the fingerprint of the enrolled person. A threshold value of the correlation of the training fingerprints is sent to the receiver to verify the presence of the enrolled person's fingerprint. Matlab simulation of the technique has been carried out to validate the proposed technique. The correlation of the log polar of the enrolled fingerprint with the log polar of the target and anti-target fingerprints has been used to authenticate the transmitted original face image at the receiver side.

Key-Words: - Digital holography, Multiple biometrics, Biometric encryption, Encryption, Decryption

1 Introduction

Security of data is a major concern in modern society, especially given the utilisation of digital techniques in the creation, editing and distribution of sensitive data [1]. The wide usage of images for many industrial or commercial purposes increases the interest in the security of images. In real-time applications, optics is very useful because of the distinct advantage of processing two dimensional complex data in parallel and carry out time costly operations at great speeds. Various optical methods have been proposed to secure the images [2-8]. Javidi *et. al.* proposed the double random phase encoding method in which two random phase masks have been used at the input and the Fourier plane [2]. In recent years, digital holography has been introduced in the security system to digitize the whole encryption systems. Digital holographic system is devoid of chemical or physical developing of the holographic plates needed after exposure [4-8]. Digital holographic systems can be described as an opto-electronic system, in which a hologram is recorded optically by multiplexing the encrypted image with the reference wave by using a CCD camera. This hologram is stored in the computer memory and reconstructed digitally. Javidi *et. al.* proposed a security system that combines the double-random phase encoding encryption system with the digital holographic system [4]. Although, the digital holography based techniques enhances the security of the system but these techniques do not have an option of authentication.

Authentication can be added in a system by using biometric of the user. So, the biometric based technologies are gaining more attraction because of secure authentication [9-14]. A biometric is defined as a unique, measurable, biological characteristic or trait for automatically recognizing or verifying the identity of a human being. Some of the most common physical biometric patterns analyzed for security purposes are the fingerprint, hand, eye, face, and voice [9]. A new method, biometric encryption has been proposed in which a PIN or a cryptographic key securely binds to a biometric, so that neither the key nor the biometric can be retrieved from the stored template. The key is re-created only if the correct live biometric sample is presented on verification [10]. Recently, some new techniques for image encryption based on biometrics have been proposed [11-14]. In all these methods, biometrics is used to authenticate the images. Optical security system based on the biometrics using holographic storage technique with a simple data format has also been proposed [12]. Kim *et al.* proposed a digital

holographic security system that combines the digital holographic memory with electrical biometrics [13]. The digital input data including a document, a picture of face, and a fingerprint are spatially multiplexed by random phase mask used as a decryption key.

In this paper, a new technique has been proposed in which the principle of digital holography has been combined with the biometrics of the user. In this method, a face image of the enrolled person has been encrypted by using fingerprint of the same person using digital holography. In the encryption process, a biometric template (BT) is generated by the log polar transform of the fingerprint of the enrolled person. The face image of the enrolled person has been spatially multiplexed with the phase mask generated by the BT. To make the phase mask random, jigsaw transform has been performed on the BT [15]. In the decryption process, the input face image can be extracted from the hologram using the encryption key.

2 Principle

Biometrics of the enrolled person is used to encrypt another biometric of the same enrolled person. The principle of digital holography has been used to encrypt the input face image of the enrolled person. The schematic diagram of the encryption process of the proposed technique is shown in Fig. 1. This technique consists of two steps. First, E_1- generation of the phase mask and second E_2- recording of the hologram. In the first step, a phase mask has been generated by using the fingerprint of the enrolled person. This is explained in detail in section 2.1. An interference of the input image with the phase mask generated by E_1 step has been obtained, which is explained in detail in section 2.2.

2.1. Generation of the phase mask by using the fingerprint of the enrolled person

As shown in the E_1 stage of Fig. 1, for generation of the phase mask, a fingerprint of size 256×256 has been captured by using a CCD camera. The centre portion of the fingerprint has more precise appearance than the outer part of the fingerprint. Rotation and scaling is also less dominant in the centre of the fingerprint. So the centre portion of the fingerprint has then been cropped. The problem of rotation and scaling is still associated with the fingerprint. These problems can be reduced by using the fingerprint in log polar domain. So the fingerprint in log polar domain has been used to generate the phase mask.

2.1.1 Log Polar Transform

The log-polar transform is a space-invariant image representation which is used to eliminate the effects of scale and rotation in an image. The log-polar transformation is a mapping of an image from the cartesian plane *(x,y)* to the log-polar plane ($log\ \rho,\theta$) [14]. The fingerprint in the log polar domain is called the biometric template (BT). The phase mask is then generated by phase encoding of the obtained BT. As shown in E_1 stage of Fig. 1 the obtained BT has symmetry due to the symmetry in the fingerprint. It can not provide the randomness in the obtained phase mask. The phase mask has been randomized by performing the Jigsaw transform (JT) of the Biometric template. The JT also has an additional property of eliminating the sharp discontinuity of the edges because of scrambling of high-frequency with lower frequencies.

2.1.2 Jigsaw Transform

The JT is an invertible, unitary and energy conserving transform. The JT (J{}), is defined as juxtaposes of different section of an image [15] according to some permutation. Therefore, no sharp discontinuities will occur due to the juxtaposition process. In this case, the image is divided into 64x64 blocks of size 4x4 pixels. These blocks are then repositioned relative to each other according to some permutations. A JT is represented by any particular index b, as $J_b\{\}$ and its inverse is $J_{-b}\{\}$ where 'b' is some permutation. This permutation also acts as an additional key for the system.

This jigsaw transformed BT has been phase encoded. This phase mask then acts as a random phase mask.

$$F(\log\rho,\theta)\rightarrow LogPolar(F(x,y)) \quad (1)$$

$$J\{F(\log\rho,\theta)\}=jigsaw(F(\log\rho,\theta)) \quad (2)$$

$$P(\log\rho,\theta)=\exp[i\pi J\{F(\log\rho,\theta)\}] \quad (3)$$

where *F(x,y),* $F(\log\rho,\theta)$ and $P(\log\rho,\theta)$ are the fingerprint in the cartesian domain, log polar domain or BT and phase mask respectively. $P(\log\rho,\theta)$ is the key for the encryption process.

2.2 Encryption of the input face image by using digital holography

In stage E_2 of the Fig. 1, a hologram is obtained digitally. In this stage a hologram is obtained by multiplexing the input face image with the phase mask. Let *(x, y)* denote the space coordinates, and *(u, v)* the coordinates in the Fourier domain. I*(x, y)* is a

real valued original face image to be encrypted. A random phase mask $R(x, y) = \exp(i2\pi n(x))$ is generated by using rand generator in Matlab platform where *n(x)* is a white sequence uniformly distributed in *[0, 1]*. The input face image is multiplied by the random phase mask (RPM) *R(x, y)* and then Fourier transformed. RPM has been generated by the rand generator in Matlab platform.

$$A(u,v) = FFT\{I(x,y) \times R(x,y)\} \quad (4)$$

An interference pattern is obtained by multiplexing of *A(u,v)* with $P(\log\rho,\theta)$ as shown in Fig. 1. The intensity of the digital hologram created by interfering two waves *A(u,v)* and *P(log(ρ,θ)* is given as:

$$H = \left|A(u,v) + P(\log\rho,\theta)\right|^2 \quad (5)$$

$$H = \left|A(u,v)\right|^2 + \left|P(\log\rho,\theta)\right|^2 + A(u,v)P(\log\rho,\theta)^* + A(u,v)^* P(\log\rho,\theta) \quad (6)$$

$$H = \left|\{I(u,v) \otimes R(u,v)\}\right|^2 + \left|P(\log\rho,\theta)\right|^2 + \{I(u,v) \otimes R(u,v)\}P(\log\rho,\theta)^* + \{I(u,v) \otimes R(u,v)\}^* P(\log\rho,\theta) \quad (7)$$

where H is the obtained encrypted hologram. *I(u ,v)* and R*(u, v)* are the input face image and RPM in the frequency domain. The BT, the random phase mask and the permutation of the JT are the keys for the technique. These keys have to be transmitted along with the encrypted hologram to the receiver side.

In the decryption process in order to extract the input face image from the encryption hologram, the DC terms are first removed which are the power spectrum of the object beam and the phase mask. The holographic data obtained after removing the DC terms are as follows:

$$H' = \{I(u,v) \otimes R(u,v)\}P(\log\rho,\theta)^* + \{I(u,v) \otimes R(u,v)\}^* P(\log\rho,\theta) \quad (8)$$

By using the received BT and the permutation of the JT, the same phase mask $P(\log\rho,\theta)$ has been generated in the decryption process by using Eqn 3.

The first term has been extracted from the obtained holographic data and then multiplied by the phase mask. An inverse Fourier transform has been performed on this term to recover the original function as given below:

$$\{I(u,v) \otimes R(u,v)\}P(\log\rho,\theta)^*\} \times P(\log\rho,\theta)$$

$$IFT\{I(u,v) \otimes R(u,v)\} = \{(I(x,y) \times R(x,y)\} \quad (9)$$

where '*IFT*' denotes the inverse Fourier transform. The result has been multiplied by the conjugate of the RPM to reject the effect of the introduction of the RPM in the input plane which is given as:

$$(I(x,y) \times R(x,y)\} \times R(x,y)^* = I(x,y) \quad (10)$$

The fingerprint can be reconstructed from the inverse log polar transform of the obtained BT as given below:

$$F(x,y) \rightarrow InverseLogPolar(F(\log\rho,\theta)) \quad (11)$$

The simulations results have been incorporated to validate the proposed technique.

3 Simulation results

A computer simulation has been carried out on the Matlab platform in order to support the proposed idea of digital holography using biometrics. The simulation results are given in Fig. 2. The face image of the enrolled person of size 100×100 has been captured and is shown in Fig. 2a. A RPM of size 100×100 is generated by using rand generator in Matlab platform. The RPM, generated by the random numbers is shown in Fig. 2b. Another biometric image is the fingerprint image of right side loop of size 256×256. This is shown in Fig. 2c. The zero padded fingerprint has been transformed into the log polar domain and is called BT. This is shown in Fig. 2d. The BT has then been jigsaw transformed. JT is performed by dividing the BT into 64×64 blocks of pixel size 4×4. This is shown in Fig. 2e. The phase encoding of the jigsawed BT has been done to generate the phase mask. The generated phase mask is shown in Fig. 2f.

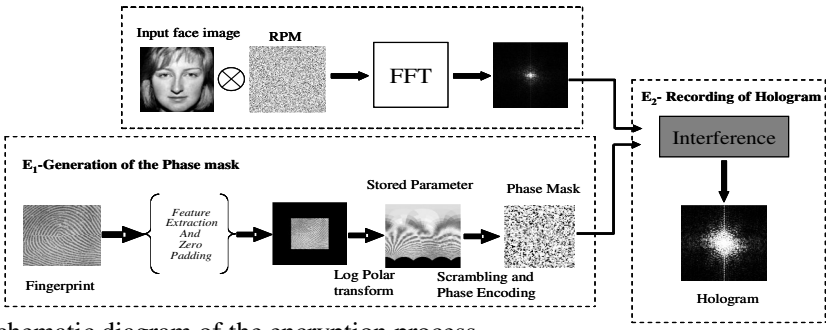

Fig.1: Schematic diagram of the encryption process.

The Fourier spectrum of the input face image multiplied by RPM has been taken. This Fourier spectrum has been multiplexed by the generated phase mask. The obtained encrypted hologram is shown in Fig. 2g. The BT and the permutation of the JT are the keys for the technique. These keys have to be transmitted along with the encrypted hologram to the receiver side. In the decryption process the encrypted hologram has been reconstructed numerically. First, the phase mask has been generated by the obtained BT. The encrypted hologram has been multiplied by the conjugate of the phase mask. The obtained data has been inverse Fourier transformed and multiplied by the conjugate of the RPM to reconstruct the original face image. The reconstructed document is shown in Fig. 2h.

To evaluate the reliability of this algorithm the mean square error (MSE) has been calculated. The MSE can be defined as:

$$MSE = \frac{1}{N \times N} \sum_{i=1}^{N} \sum_{j=1}^{N} (|I_1(i,j) - I_2(i,j)|^2) \quad (12)$$

where $I_1(i, j)$ and $I_2(I, j)$ are pixel values at location (i, j) for the input image and the output images respectively. The $N \times N$ represents the total number of pixels of the image. The MSE between the input face image and the encrypted hologram and the MSE between the input face image and the reconstructed document image has been calculated and which are 2.9186e+003 and 0.0802 respectively.

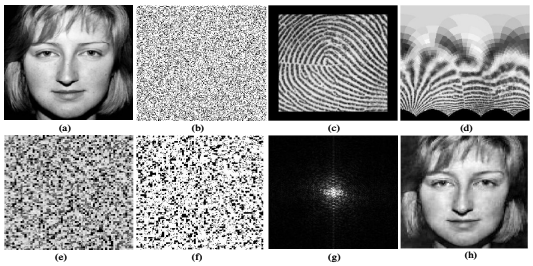

Fig.2: Results of computer simulation: (a) Original face image, (b) RPM, (c) fingerprint of the enrolled person, (d) log polar plot of the fingerprint, (e) jigsaw transformed log polar fingerprint image, (f) phase mask generated by the fingerprint, (g) encrypted hologram, (h) Reconstructed document.

4 Authentication of the Original Document

In the proposed technique, a face image of the enrolled person has been encrypted digitally by using the fingerprint of the same person. A detailed study has been done to authenticate the transmittance of the right encrypted face image of the enrolled person. So the correlation of the target fingerprint with the rotated and scaled version of the target and anti-target fingerprint has been calculated. These correlation values have also been sent to the receiver along with the encrypted image and the BT. At the verification side, after the retrieval of the face image correlation of the BT with the live fingerprint has been calculated. The higher correlation value will assure the transmittance of the right encrypted image or presence of the right fingerprint of the enrolled person in the verification. A lower value of correlation will result only if the encrypted image and BT is exchanged or if the right database of the enrolled person is not present on verification.

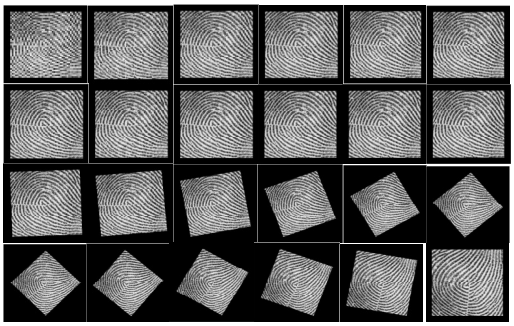

Fig. 3 A set of rotated and scaled version of the target fingerprint

For this purpose a dataset of rotated and scaled version of the target fingerprint has been obtained by rotating and scaling of the BT respectively. This dataset is shown in Fig. 3. Similarly, a set of anti target fingerprints has been captured and zero padded as explained in section 3. Then the log polar transform has been performed. Some of the anti target fingerprints and their images in log polar domain are shown in Fig.4. The correlation of BT with the log polar of the target fingerprints and the correlation of BT with the log polar of the anti target fingerprints are shown in Fig. 5a. The correlation of BT with the log polar of rotated version of the target fingerprint and the correlation of BT with the log polar of the rotated version of the anti target fingerprint are shown in Fig. 5b. The correlation of BT with the log polar of the scaled version of the target fingerprint and the correlation of BT with the log polar of the scaled version of the anti target fingerprint are shown in Fig. 5c. A threshold value has been calculated by taking the mean of the minimum value of the correlation of the BT with the target fingerprint and the maximum value of the correlation of the BT with the anti target fingerprint. The obtained threshold values are sent to the receiver side. After the retrieval of the input face image by decrypting the encrypted hologram at the receiver side, the

retrieved document can be verified.

` In order to verify the original data, the BT is correlated with the live fingerprint of the enrolled person. If the correlation value is higher than the threshold value, the presence of the right face image of the enrolled person is authenticated. A lower correlation value indicates the presence of an unauthorized person.

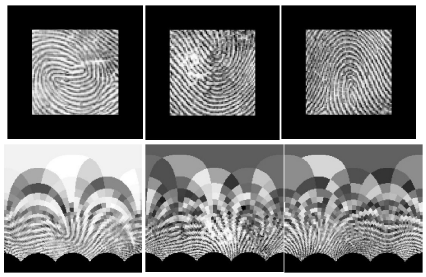

Fig.4: Anti target fingerprints and their log polar plots.

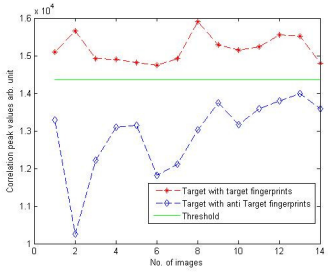

Fig.5a: Correlation of the BT with the log polar of the target fingerprint and log polar of the anti target fingerprint.

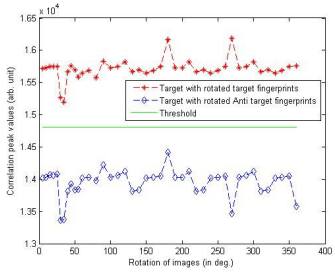

Fig.5b: Correlation of the BT with the log polar of the rotated target fingerprint and log polar of the rotated anti target fingerprint.

5 Conclusion

A new biometric based encryption technique using the principle of digital holographic security system has been proposed. In this method, a biometric of an enrolled person has been secured by using another biometrics of the enrolled person. The face image of the enrolled person can be spatially multiplexed by a phase mask. This phase mask has been generated by the fingerprint of the enrolled person. The use of the fingerprint is highly restricted by the rotation and scaling of the fingerprint. In order to overcome the problem of rotation and scaling of the fingerprint the log polar transform of the fingerprint has been used. The use of the phase mask generated by the fingerprint of the enrolled person authenticates the presence of the right input face image. The phase mask generated by the fingerprint has less randomness due to the symmetry of the fingerprint. To randomize the phase mask the jigsaw transform has been performed on the fingerprint in the log polar domain. Along with the randomization of the fingerprint image the Jigsaw transform provides permutation as an additional key to the system. This method has advantage over other digital holographic security system due to its capability of authentication on the verification as the biometric template (BT) has also been sent along with the hologram. The correlation of the BT with the log polar of the target and the log polar of the anti target fingerprints has been calculated. The threshold value of the correlation of the training fingerprint is sent to the receiver side to verify the presence of the enrolled person's fingerprint. Matlab simulation of the technique has been done to validate the proposed technique.

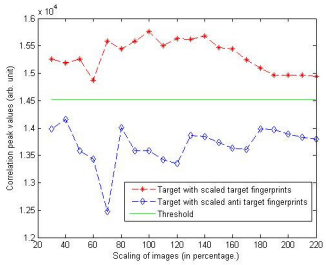

Fig.5c: Correlation of the BT with the log polar of the scaled target fingerprint and log polar of the scaled anti target fingerprint.

References:

[1] Hoque S, Fairhurst M, Howells G, Deravi F. Feasibility of generating biometric encryption keys. Elect Lett 2005;41:309-311.

[2] Refregier P, Javidi B. Optical image encryption based on input plane and Fourier plane random encoding. Opt Lett 1995;20:767-769.

[3] Zhang Y, Wang B. Optical image encryption based on interference. Opt Lett 2008;33:2443-2445.

[4] Javidi B, Nomura T. Securing information by use of digital holography. Opt Lett 2000;25:28-30.

[5] Tajahuerce E, Javidi B. Encrypting three-dimensional information with digital holography. Appl Opt 2000;39:6595-6601.

[6] Zhu B, Zhao H, Liu S. Image encryption based on pure intensity random coding and digital holography technique. Optik 2003;114:95-99.
[7] Arizaga R, Henao R, Torroba R. Fully digital encryption technique. Opt Commun 2003;221:43-47.
[8] Yu L, Cai L. Multidimensional data encryption with digital holography. Opt Commun 2003;215:271-284.
[9] Soutar C, Roberge D, Stoianov A, Gilroy R, Vijaya Kumar BVK. Biometric encryption™. http://www.bioscrypt.com;1999.
[10] Cavoukian A, Stoianov A. Biometric encryption. P Information and Privacy Commissioner/Ontario;2007.
[11] Saini N, Sinha A. Optics based Biohashing using joint transform correlator, Opt Comm 2010;283:894-902.
[12] An JW. Optical security system based on the biometrics using holographic storage technique with a simple data format. Chinese Phys Lett 2006;23:116-118.
[13] Kim J, Choi J, An J, Kim N, Lee K. Digital holographic security system based on random phase encoded reference beams and fingerprint identification. Opt Comm 2005;247:265-274.
[14] Saini N, Sinha A. Optics based Biometric encryption using log polar transform, Opt Comm 2010; 283:34-43.
[15] Hennelly B, Sheridan JT. Optical image encryption by random shifting in fractional Fourier domains. Opt Lett 2003;28:269-271.