Design of Cascaded Phase Keys for Hierarchical Security System

Chia H. Yeh, Hsuan T. Chang[†]*, Hung C. Chien, & Chung J. Kuo*

Signal and Media (SAM) Laboratory
Department of Electrical Engineering
National Chung Cheng University
Chiayi, 62107 Taiwan

[†]Department of Electrical Engineering
National Yunlin University of Science and Technology
Touliu Yunlin, 64002 Taiwan

Abstract

An image cryptosystem based on multiple phase-only masks is proposed. The proposed cryptosystem is a hierarchical security system that can use multiple phase keys to retrieve different amounts of data. In addition to the sequential order of the phase keys, the distance parameters among the phase keys are introduced to increase the system security. Even when an illegal user steals all the phase keys, the system cannot be broken without the correct sequential order and the distance parameters. On the other hand, the proposed system can verify the identities of the persons by the cascaded structure for the phase keys to generate different verification images. Simulation results are further demonstrated to verify the proposed method.

OCIS codes: 100.3020 100.5070 070.2580

Keywords: image encryption, hierarchical security system, phase retrieval, verification.

Please send correspondence to Prof. Hsuan T. Chang, E-mail: htchang@pine.yuntech.edu.tw

March 16, 2002

1 Introduction

Information security becomes very important in data storage and transmission with the fast progress of the data exchange in the electronic commerce. Optical techniques for data security[1−5] have received great deal of the attention since last decade. The characteristics of fast computing and parallelism for optics are very useful in real-time applications. Optical information can be hidden in the phase or the amplitude forms. Both the amplitude and the phase information of the encrypted data are recorded in conventional optical encryption techniques. If encrypted data can be phase or amplitude only, the recording and storage should be easier.[6] Since the phase information is more important than the amplitude information,[7] the phase information is often chosen to encrypt and retrieve data.

The phase information is typically recorded by the phase-only mask in which we can assign the arbitrary phase and constant amplitude transmittance. The phase-only mask for diffracting its input light to any desired output position is named as a diffractive optical element and can be achieved by the hologram technique or the fabrication process.[8] The projection onto constraint set (POCS) technique[9,10,14−17] and the far filed assumption[13] are usually used to design the phase-only mask. This technique employs the Fourier transform[11−13] to model the formation of the output diffraction pattern of the phase-only masks. On the other hand, the transmittance of the phase-only mask and its output light distribution must satisfy both the input- and output-domain constraints. The input domain constraint usually is the constant amplitude transmittance, while the output domain constraint is regarded as the maximum allowable absolute error between the desired and the actual diffraction pattern.

The relationships among the primary user and the others are usually determined by the authority of the data-access control in a hierarchical security system. The users in different levels have different numbers of phase keys to access the hierarchical security system to obtain the information, and the high-level users can access the information for the lower-level ones shown in Fig. 1. With wide applications of the security systems, the data-access control of the hierarchical security system is very important. Unfortunately, conventional optical systems hardly get involve with these applications. In this paper, a new scheme for the hierarchical security system is proposed based on the cascaded phase-only masks, which can be used to retrieve different target images. Considering the case of the n phase keys in the system, the n optimized phase-only masks can be individually found for n different target images or n different amounts of information contents by the POCS algorithm. Here, the ith phase key is the phase difference of the ith and the $(i-1)$th optimized phase-only masks. Distance parameters among n phase keys are introduced instead of being together with each other to increase the system security. Consequently, only the phase keys cannot be used to access the system without the distance parameters. Users of different levels need their corresponding number/order of the phase keys and correct distance parameters to retrieve the corresponding information or perform the verification.

This paper is organized as following. Section 2 explains the concept of our proposed scheme. Section 3 shows simulation results. Conclusions are finally made in Section 4.

2 Proposed System

2.1 Basic Architecture

The optimized phase-only mask such that the output diffraction pattern (target image) is best matched to the desired one can be found to achieve the goals in the previous section. Figure 2 shows the basic architecture of the proposed system which is composed of the phase-only mask with the optical transmittance function (OTF, denoted as $G(\cdot,\cdot)$), an input plane I where the phase-only mask is located at, a Fourier transform lens, and an output plane O that is at the focal length with distance $L/2$ behind the lens. Let z axis be the optical propagation axis and the coordinates of the input and the output planes be (x,y) and (f_x,f_y), respectively. The light distributions at the input and the output plane are denoted by $U_I(x,y)$ and $U_O(f_x,f_y)$, respectively. The expression for $U_I(x,y)$ and $U_O(f_x,f_y)$ is shown as bellow.

$$\begin{aligned} U_I(x,y) &= A_I(x,y) \times P_I(x,y) = A_I e^{j\phi_I(x,y)}, \qquad (1)\\ P_I(x,y) &= \exp[j\phi_I(x,y)], \\ U_O(f_x,f_y) &= A_O(f_x,f_y) \times P_O(f_x,f_y) = A_O e^{j\phi_O(f_x,f_y)}, \qquad (2)\\ P_O(f_x,f_y) &= \exp[j\phi_O(f_x,f_y)], \end{aligned}$$

where A_I and A_O denote the amplitude of U_I and U_O; ϕ_I and ϕ_O represent the phase of U_I and U_O, respectively. Since the Fourier transform is used as the mathematical tool to model the light propagation and performed by the lens,[13] the relationship between the light distributions $U_I(x,y)$ and $U_O(f_x,f_y)$ is expressed by,

$$U_O(x,y) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} U_I(x,y)G(x,y)\exp[j\frac{2\pi}{\lambda L}(xf_x + yf_y)]dxdy. \qquad (3)$$

The optimized phase-only mask for one target image can be determined by the POCS algorithm whose block diagram is shown in Fig. 3. The procedures for the iteration process are given as follows.

1. Given an output diffraction pattern (target image), find the corresponding OTF of the phase-only mask by the inverse Fourier transform.

2. Fix the amplitude transmittance $A_I(x,y)$ of the phase-only mask to be unity.

3. Apply the output-domain constraint to the new output diffraction pattern.

4. Repeat Steps 1 to 3 until the phase-only mask or the diffraction image does not change.

Let $P_I(x,y)$ denote the optimized phase-only mask for the target image. First, the POCS algorithm is employed to find n phase-only masks $P_{I,i}(x,y)$ for n different target images, where $i = 1, \cdots, n$. To construct a hierarchical security system, n phase keys are determined by calculating the n corresponding phase differences from the neighboring optimized phase-only masks, $P_{I,i}(x, y)$ and $P_{I,i-1}(x, y)$. The basic optical setup of the proposed system is similar to that shown in Fig. 2 except that there are n phase keys in the input plane. The ith phase key K_i is the phase difference between two neighboring optimized phase-only masks and defined by,

$$K_i = \frac{P_{I,i}(x, y)}{P_{I,i-1}(x, y)} = \exp[j(\phi_{I,i}(x, y) - \phi_{I,i-1}(x, y))]. \tag{4}$$

The ith phase key K_i combines the phase information of the ith and the $(i - 1)$th optimized phase-only masks and its phase distributions is quasi-random. In the basic architecture, the higher-level users must own more phase keys (the phase keys must be placed in a correct order) to retrieve more target images than that of the lower-level ones. Once a plane wave is incident to the input plane I, the retrieved target image under nth phase keys in the output plane O is given by

$$\begin{aligned} U_{O,n}(f_x, f_y) &= \mathrm{FT}\{K_1 \times K_2 \times \cdots \times K_n\} \qquad (5) \\ &= \mathrm{FT}\{\exp[j(\phi_{I,1}(x, y) - \phi_{I,0}(x, y) + \phi_{I,2}(x, y) - \phi_{I,1}(x, y) + \cdots + \\ &\qquad \phi_{I,n}(x, y) - \phi_{I,n-1}(x, y))]\} \\ &= \mathrm{FT}\{\exp[j\phi_{I,n}(x, y)]\} \\ &= \mathrm{FT}\{P_{I,n}(x, y)\}, \end{aligned}$$

where FT denotes the Fourier transform, $A_{I,i}(x, y) = 1$ for all i, and $\phi_{I,0}(x, y) = 0$.

2.2 Advanced Architecture

The distance parameters d_i between n phase keys are introduced to increase the system security. Figure 4 shows the advanced architecture of the proposed system. When the field traverses through an optical path distance d_i (the distance from one phase key to input plane), a substantial phase change happens shown in Fig. 5. The relationship between the initial optical filed U_I and another optical field $U_{I,i}$ behind an optical path $d_i, i = 1, \cdots, n$ is given by[18]

$$\begin{aligned} U_{I,i}(x_i, y_i) &= \int\int U(x, y) \exp[j\frac{k}{2d_i}((x - x_i)^2 + (y - y_i)^2)]dxdy \qquad (6) \\ &= U(x, y) \otimes \exp[j\frac{k}{2d_i}(x_i^2 + y_i^2)], \end{aligned}$$

where $k = 2\pi/\lambda$ (λ is the wavelength) and $\otimes$ denotes the convolution operation. Here, the impulse response of the space distance is defined by $h(d_i) = \exp[j\frac{k}{2d_i}(x_i^2 + y_i^2)]$. Let the phase key K_i has a distance d_i left from the input plane I and $d_i > d_{i-1}$ for all i. The phase keys K_i' after introducing distance parameters can be expressed as,

$$\begin{aligned} K_1' &= K_1 \otimes h(-d_1), \qquad (7) \\ K_2' &= ((K_2 \otimes h(-d_1)) \times \overline{K'}_1) \otimes h(-(d_2 - d_1)), \\ K_3' &= (((K_3 \otimes h(-d_1)) \times \overline{K'}_1) \otimes h(-(d_2 - d_1)) \times \overline{K'}_2) \otimes h(-(d_3 - d_2)), \\ \vdots &= \qquad\qquad \vdots \\ K_n' &= (\cdots(((K_n \otimes h(-d_1)) \times \overline{K'}_1) \otimes h(-(d_2 - d_1)) \times \overline{K'}_2) \otimes h(-(d_3 - d_2)) \\ &\quad \cdots \times \overline{K'}_{n-1}) \otimes h(-(d_n - d_{n-1})), \end{aligned}$$

where $\overline{K'}_i$ denotes the complex conjugate of K_i'. Each of n phase keys is modified by considering the corresponding distance factor according to the equations above. In this advanced architecture, the high-level users simultaneously own all phase keys, the correct order of the phase keys, and the correct distance parameters to retrieve all of the target images. Once a plane wave is incident to the input plane I, the retrieved ith target image under n phase keys in the output plane O is given by,

$$\begin{aligned} U_{O,i}(f_x, f_y) &= \mathrm{FT}\{((\cdots(K_i' \otimes h(d_i - d_{i-1}) \times K_{i-1}') \otimes h(d_{i-1} - d_{i-2}) \cdots \times K_1') \otimes h(d_1)\} \\ &= \mathrm{FT}\{K_i\} \qquad (8) \\ &= \mathrm{FT}\{\exp[j\phi_{I,i}(x, y)]\} \\ &= \mathrm{FT}\{P_{I,i}(x, y)\}, \end{aligned}$$

where $A_{I,i}(x, y) = 1$ for all i. The order of n correct phase keys and n distance parameters should be employed to obtain the nth target image; therefore, illegal users without all the information cannot retrieve the target images. Our proposed system thus can be employed not only in the hierarchical security system but also in the optical verification and security sharing systems.

3 Simulation Results

In the computer simulation, three test images (Lena, Jetplane, and Baboon) shown in Fig. 6 are used as the target images of the hierarchical security system in levels one, two and three, respectively. Each image used for computer experiments has 128×128 pixels and each pixel has 8-bit grayscale resolution. The sizes of optimized phase-only masks and phase keys are also 128×128.

The iteration process proceeds based on the steps mentioned in Section 2. Then, three optimized phase-only masks P_1 to P_3 for three target images can be obtained by the POCS algorithm shown in Figs. 7(a) to 7(c). Three phase keys for the basic architecture can be derived from Eq. 4 and their phase distributions are shown in Figs. 8(a) to 8(c). Here, the range of the phase distribution, $[0, 2\pi]$, is normalized into the range of the grayscale, $[0, 255]$. Figure 9 shows three retrieved images when correct phase keys and order in the hierarchical security system are used. The peak-to-noise ratio (PSNR) of three retrieved images (compared with original three images) is shown in Table 1.

Considering the advanced architecture in which three distant parameters among three phase keys are introduced, three phase keys are located from input plane with distances d_1, d_2, and d_3, respectively. In our simulation, the distance parameters d_1, d_2 and d_3 are 5 mm, 10 mm, and 15 mm, respectively, and the wavelength is 850 nm. Three phase keys can be derived from Eq. 7 are shown in Fig. 10. Figure 11 shows three retrieved images when correct phase keys and its corresponding distance parameters in which the advanced architecture are used. The PSNR of three retrieved images (compared with original three images) is also shown in Table 1. The images retrieved from the advanced architecture have slightly worse quality than that from the basic architecture shown in Table 1.

Figure 12 shows the retrieved images without second phase key in the basic architecture. Users cannot retrieve target image in the level three without all phase keys. Figures 13(a) to 13(c) show the retrieved target images with three incorrect distance parameters ($d_1 = 6$ mm, $d_2 = 9$ mm, and $d_3 = 16$ mm) in the advanced architecture. The user cannot retrieve any information in all levels without the correct distance parameters. From the simulation results, the proposed system is safe and secure for data protection or verification.

4 Conclusion

In this paper, a hierarchical security system based on cascaded phase keys which are designed to perform hierarchical data-access control for different target images is proposed. The proposed method can achieve higher security since the phase keys must have correct corresponding order and distance parameters. The system is safe even when illegal user steals the all phase keys but with incorrect order and distance parameters. The more phase keys are owned, the more secret information can be obtained. Besides from the application of hierarchical data encryption, the system can also provide the verification of the identity of the persons. According to simulation results, our proposed system is effective and efficient for the hierarchical security system and the optical verification.

Acknowledgment

This research was partly supported by the National Science Council, Taiwan under contracts NSC-89-2218-E-194-019 and NSC -90-2213-E-224-030.

References

[1] P. Refregier & B. Javidi, "Optical image encryption using input plane and Fourier plane random encoding," *Optics Letters*, **20** pp. 767–769, 1995.

[2] R.K. Wang & I.A. Watson, "Random phase encoding for optical security," *Optical Engineering*, **35** pp. 2464–2469, 1996.

[3] Y. Li, K. Kreske & J. Rosen, "Security and encryption optical systems based on a correlator with with significant output images,"*Applied Optics*, **39** pp. 5295–5301, 2000.

[4] J.W. Han, C.S. Park, D.H. Ryu & E.S. Kim, "Optical image encryption based on XOR operation," *Optical Engineering,* **37** pp. 47–54, 1999.

[5] T.S. Chen, C.C. Chang & M.S. Hwang, "A virtual image cryptosystem based upon vector quantization," *IEEE Transactions on Image Process,* **7** pp. 1485–1488, 1998.

[6] N. Towghi, B. Javidi & Z. Luo, "Fully phase encryption image processor," *Journal of Optical Society of America, Part A*, **16** pp. 1915–1927, 1999.

[7] M. H. Hayes, "The reconstruction of a multidimensional sequence from the phase or magnitude of its Fourier transform," *IEEE Transactions on Acoustic, Speech and Signal Processing,* **ASSP-30** pp. 140–154, 1982.

[8] C. J. Kuo and M. H. Tsai, Three dimensional holographic imaging, John Wiley and Sons, Inc. New York, 2002

[9] A. Papouli, "A new algorithm in spectral analysis and band-limited extrapolation," *IEEE Transactions on Circuits & Systems,* **22** pp. 735–742, 1975

[10] G. Strang, *Introduction to Applied Mathematics,* Wellesley, 1986.

[11] F. Wyrowski & O. Bryngdahl, "Iterative Fourier-transform algorithm applied to computer holograms," *Journal of Optical Society of America, Part A,* **5** pp. 1058–1065, 1988.

[12] J.R. Fienup, "Iterative method applied to image reconstruction and to computer-generated holograms," *Optical Engineering,* **19** pp. 297–306, 1980.

[13] J.W. Goodman, *Introduction to Fourier Optics,* 2nd Ed., Chapter 4, McGraw-Hill, New York, 1996.

[14] J.R. Fienup, "Phase retrieval algorithms: A comparison," *Applied Optics,* vol. 21, pp. 2758–2769, 1982.

[15] R.W. Gerchberg & W.O. Saxton, "A particular algorithm for the determination of phase from image plane picture," *Optik,* vol. 35, pp. 237–246, 1972.

[16] R.W. Gerchberg, "Superresolution through error energy reduction," *Optics Acta,* vol. 21, pp. 709–720, 1974.

[17] J. Rosen, "Learning in correlators based on projection onto constraint sets," *Optics Letters*, **18**, pp. 1183–1185, 1993.

[18] A. D. Poularilcas and S. Seely, Signals and Systems, PWS-KENT Publishing Company, Boston, 1991.

System architecture	Lena	Jetplane	Baboon
Basic	32.88 dB	32.56 dB	32.23 dB
Advanced	32.68 dB	32.42 dB	32.12 dB

Table 1: PSNR comparison of three retrieved images in the basic and advanced architectures.

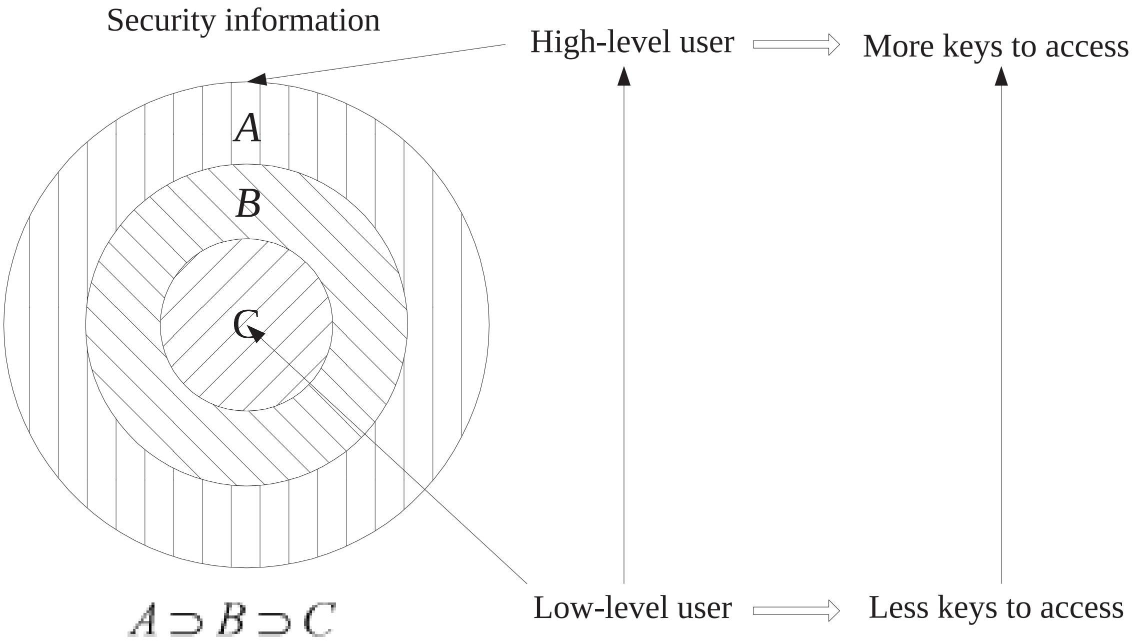

Figure 1: Data-access control in hierarchical security system.

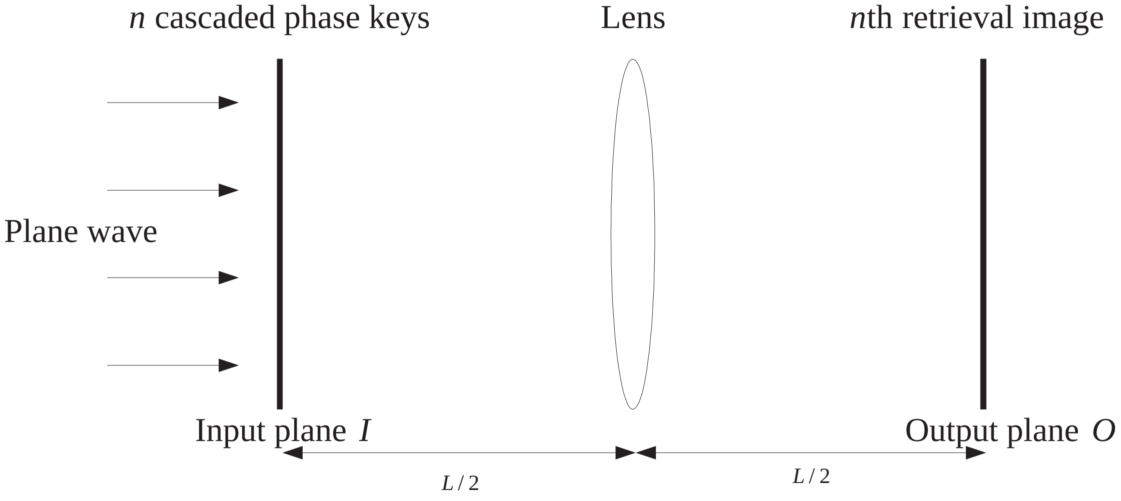

Figure 2: Optical setup of the basic architecture.

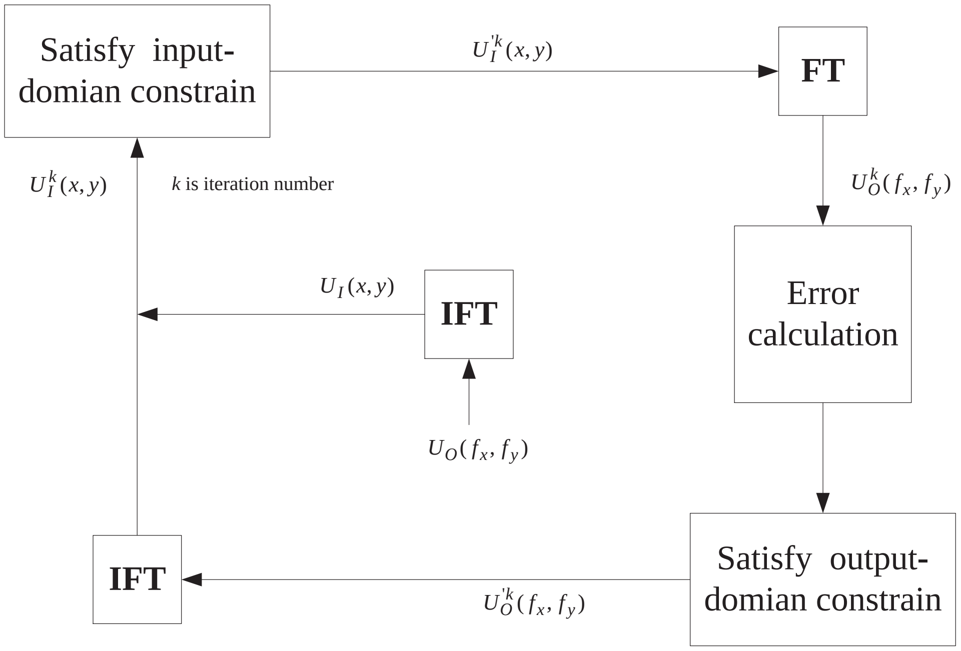

Figure 3: Block diagram of the POCS algorithm.

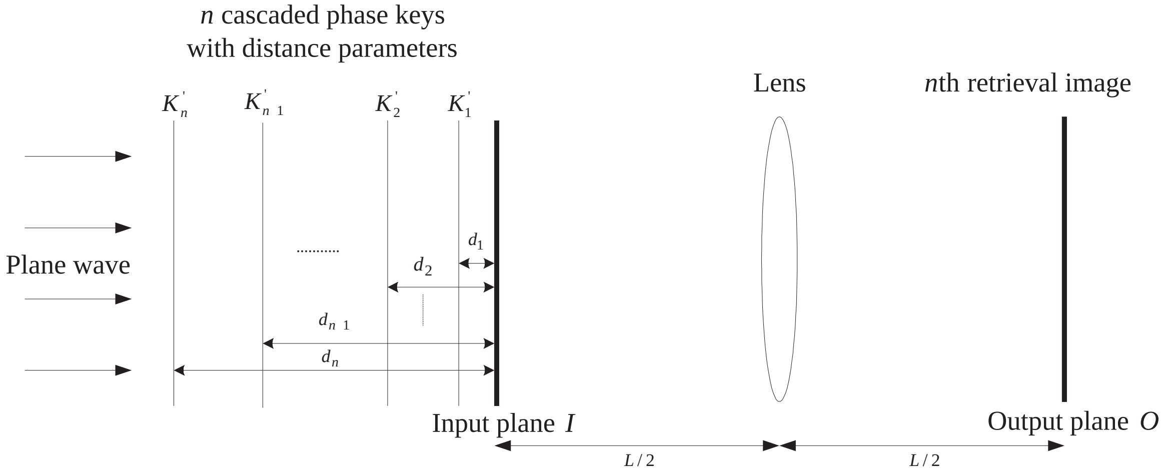

Figure 4: Optical setup of the advanced architecture.

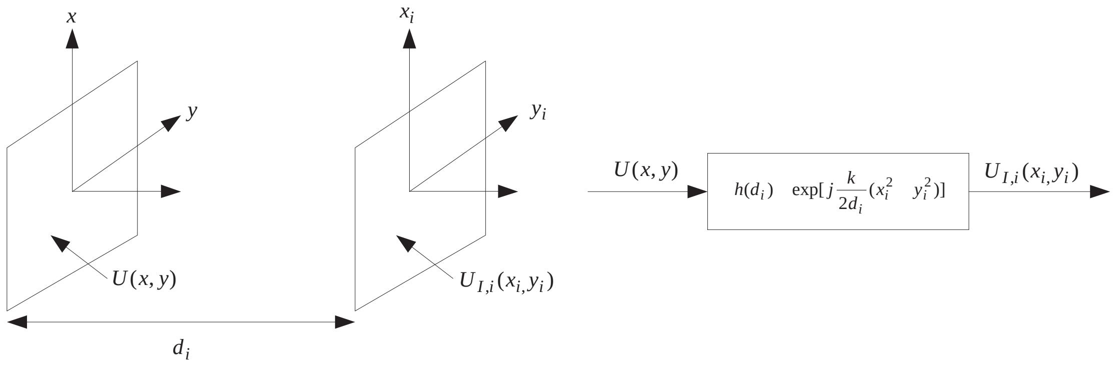

Figure 5: Schematic and operation representation of the space distance d_i.

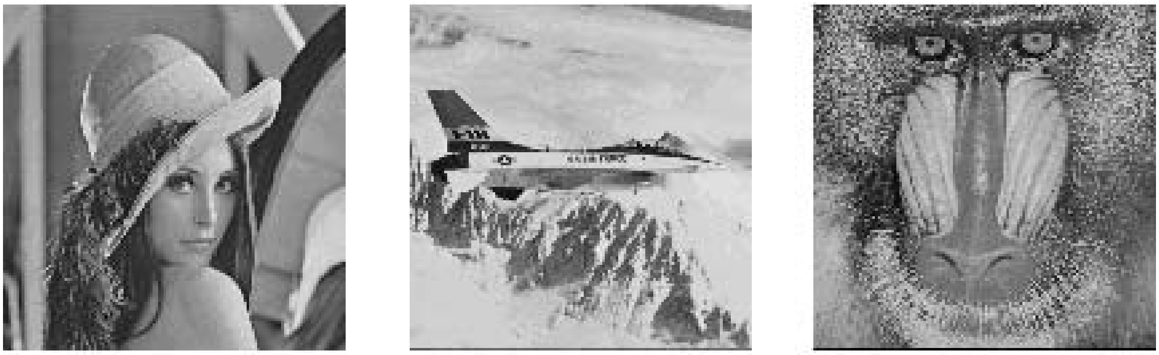

Figure 6: Three test images in levels one, two and three.

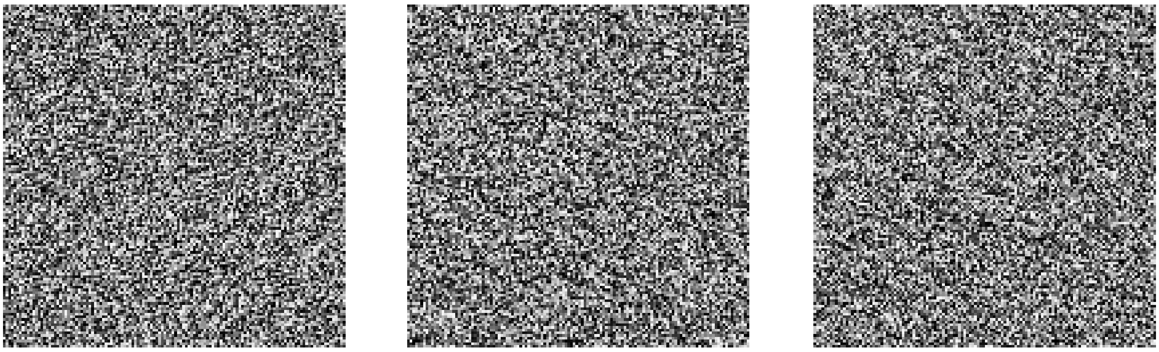

Figure 7: Phase distribution of three optimized phase-only masks P_1, P_2, P_3 generated by POCS algorithm.

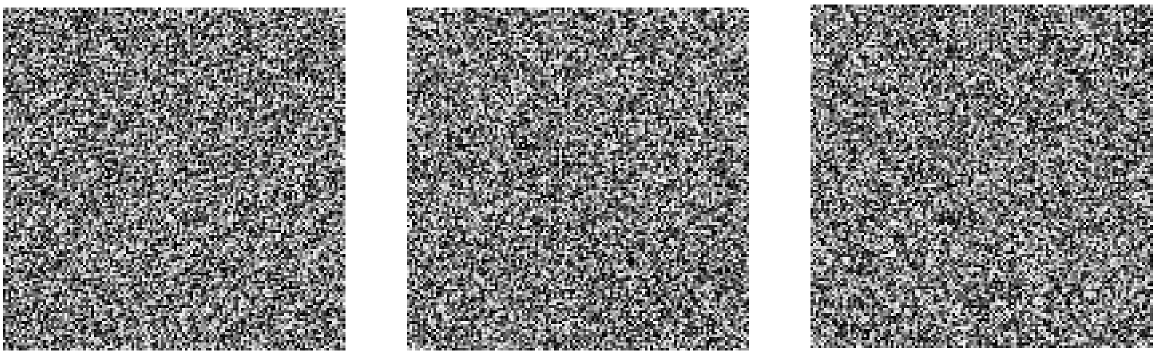

Figure 8: Phase distribution of the three phase keys $P_{I,1}, P_{I,2}, P_{I,3}$ in the basic architecture.

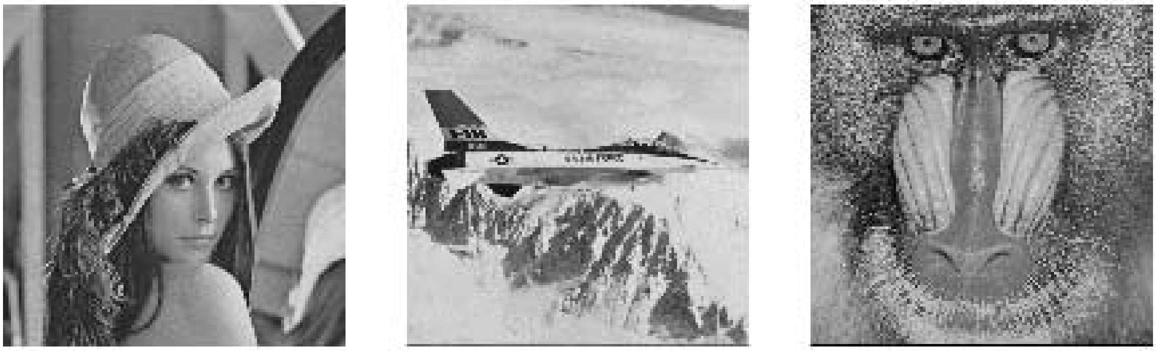

Figure 9: Retrieved images of the basic architecture in levels one, two and three.

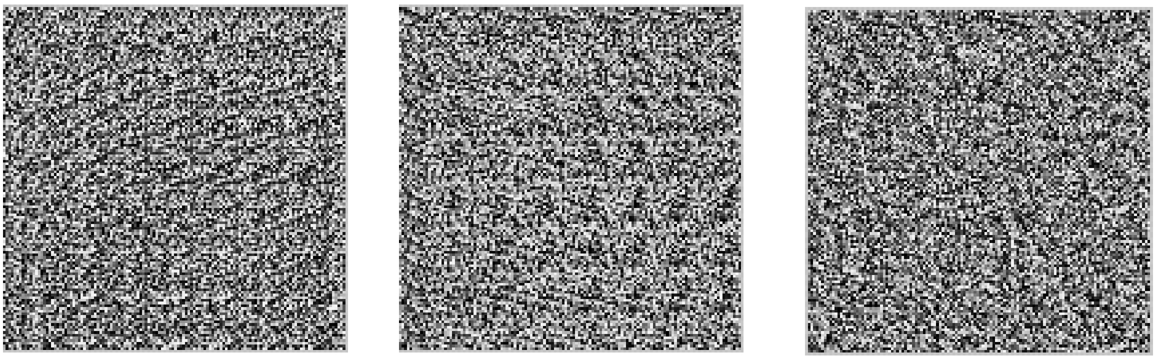

Figure 10: Phase distribution of the three phase keys $P_{I,1}, P_{I,2}, P_{I,3}$ in the advanced architecture.

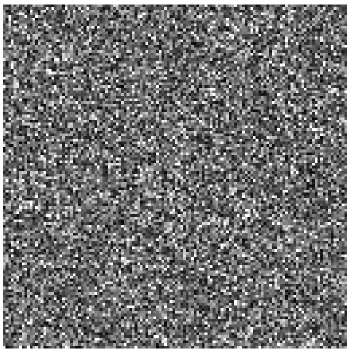

Figure 11: Retrieved image without second phase key P_2 in the basic architecture.

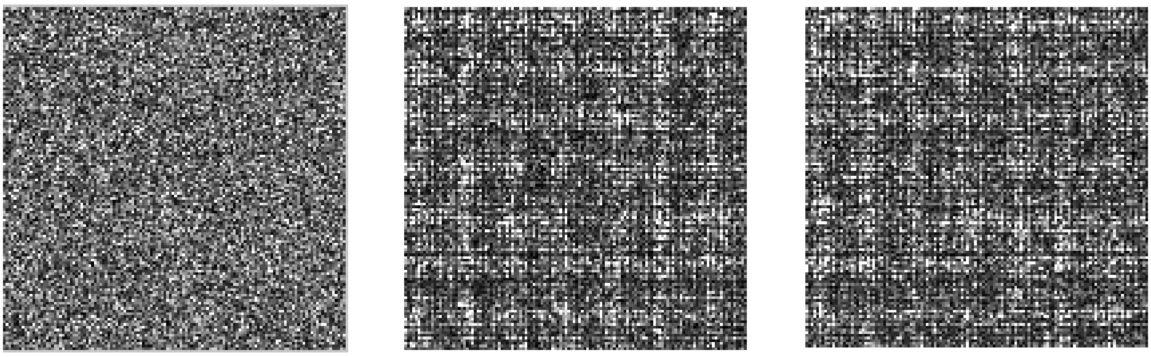

Figure 12: Retrieved images with incorrect distance parameters ($d_1 = 6$ mm, $d_2 = 9$ mm, and $d_3 = 16$ mm) in the advanced architecture.