

# Asymmetric-Image Verification for Security Optical Systems based on Joint Transform Correlator Architecture

*Hsuan T. Chang and Ching T. Chen*

Photonics and Information Laboratory  
Department of Electrical Engineering  
National Yunlin University of Science and Technology  
Touliu Yunlin, 64045 Taiwan ROC

## Abstract

In this paper, an optical asymmetric-image verification system based on the joint transform correlator architecture is proposed. An additional phase mask is attached to the spatial light modulator that displays the joint power spectrum as the amplitude information, to improve the system security and also enable the reconstruction of an asymmetric image. Two phase-only functions as keys are paired and iteratively retrieved by the use of the projection onto constraint sets and the multiple phase retrieval algorithms. In addition to the capability of reconstructing asymmetric images, the proposed architecture can also yield the better image quality for symmetric images. Simulation results are given to verify the proposed method and the dominant effects of two phase keys are discussed .

**Keywords:** optical security, joint transform correlator, image verification, phase retrieval, iteration algorithm.

March 2, 2004

# 1 Introduction

Optical joint transform correlators (JTCs) recently have shown the wide applications on optical security.<sup>1-4</sup> Two major applications are the optical image encryption<sup>1</sup> and the image verification.<sup>2</sup> As for the image encryption applications, a plain image  $f(x, y)$  attached to a phase function  $h_1(x, y)$  and another phase function  $h_2(x, y)$  as the joint input functions are placed side by side in the input plane. With the joint Fourier transform, the image can be encrypted as the joint power spectrum, which is real and non-negative and can be easily to be detected and recorded. To decrypt the plain image, a  $4-f$  correlator architecture commonly used in optical convolution is employed. The same phase functions  $h_1(x, y)$  is placed at the input plane and the encrypted data is placed in the Fourier plane. By illuminating the plane wave on the input plane, the original plain image can be detected in the output plane.

For the applications of the image verification, there is no input plain image and both the input functions  $h_1(x, y)$  and  $h_2(x, y)$  in the input plane are phase-only. That is,  $h_1(x, y) = \exp[i2\pi p_1(x, y)]$  and  $h_2(x, y) = \exp[i2\pi p_2(x, y)]$ , where both functions  $p_1(x, y)$  and  $p_2(x, y)$  are the random numbers within the range  $[0, 1]$ . Figure 1 shows the optical setup of the JTC architecture. Initially, both phase functions are randomly generated. The phase function  $h_2(x, y)$  is fixed and acts as a lock and the phase function  $h_1(x, y)$  acts as a key. To obtain a target image in the output plane for the fixed phase function  $h_2(x, y)$ , the other one  $h_1(x, y)$  is iteratively retrieved using the phase retrieval algorithms<sup>5</sup> such as the projection onto constraint set (POCS) algorithm.<sup>6</sup> For different initial phase functions of  $h_1(x, y)$ , the iterated results will be also different. Therefore, there are many possible keys that can match the single lock to reconstruct the same plain image. This property can be

used in the access control of a security system, in which only the correctly reconstructed image can verify that the user is authorized. It is also possible to retrieve different phase keys for the same phase lock to generate different target images, which can correspond to different levels of authority.

One major limitation of the method above is that only the symmetric images can be reconstructed in the output plane. This is because the joint power spectrum is real-valued and thus its Fourier transform is symmetric in the magnitude part.<sup>2</sup> The data amount in a symmetric image is only half of its size. If an asymmetric image can be reconstructed in the output plane, more target images can be assigned in designing the security system and the verification can be much easier. Another limitation comes from the low quality of the reconstructed images. The sizes of the phase functions in the input plane are much smaller than the target image. Therefore, with the POCS algorithm only the image that is an approximation of the target image can be obtained in the output plane. It is desired to reconstruct the target images with higher quality. Increasing the phase information will effectively enhance the reconstructed image quality. Finally, the security of the conventional architecture is not high enough to against the brute force method because the data amount in the phase key in the input plane is small. A larger phase mask can increase the system security because the possible combinations of the phases distributed in the mask increase exponentially with respect to its size. Therefore, higher system security can be achieved when more phase information is employed.

In order to obtain asymmetric images in the output plane, a complex function is required such that the magnitude of its Fourier transform can be asymmetric. To achieve this goal, an additional phase  $h_3(u, v) = \exp[i2\pi p_3(u, v)]$  is required to attach the original

real joint power spectrum. Therefore, in this paper we propose a new architecture, in which an additional phase mask is attached to the spatial light modulator (SLM) in the conventional JTC architectures. According to the similar idea shown in our previous work,<sup>7</sup> one of the joint phase functions in the input plane and this extra phase mask will be simultaneously and iteratively retrieved such that the target image can be constructed in the output plane. Compared with the conventional JTC architectures, the proposed method requires an additional phase mask whose size is identical to that of the SLM. That is, more information is used for reconstructing the plain image in addition to the phase functions in the input plane. Therefore, the reconstructed image is expected to obtain much better quality than that of the original JTC architecture in which only joint phase functions located in the input plane are used. Moreover, the additional phase function also increases the system security because only two pair-wised phase keys can correctly reconstruct the target image. However, an additional phase mask definitely increases the cost in building an image verification system.

The remainder of this paper is organized as follows: Section 2 describes the proposed architecture for asymmetric-image verification and the detailed procedures for the phase retrieval algorithm. The simulation results for both the asymmetric and symmetric images are given in Section 3. Finally, Section 4 concludes this paper.

## 2 The Proposed Architecture

In conventional security optical systems based on JTCs, the power spectra of joint input functions are real and non-negative. Because the Fourier transform of a real function is symmetric in the magnitude part, it can only reconstruct symmetric images in the output

plane. However, the information contained in a symmetric image is actually only half of the image size. Therefore, to increase the useful information in the reconstructed image, an asymmetric image is desired. To achieve this goal, we here propose a new architecture that is modified from and quite similar to the conventional JTC.

The optical architecture of the proposed method is shown in Fig. 2. Once a coherent plane wave is incident to the input plane, the charge-coupled device (CCD) sensor detects the joint power spectrum of both phase functions. That is, the joint power spectrum  $O'(u, v)$  is given by

$$O'(u, v) = |\text{FT}\{\exp[i2\pi p_1(x, y)] + \exp[i2\pi p_2(x, y)]\}|^2, \quad (1)$$

and then displayed in the SLM as the magnitude (transmittance) form. By Fourier transforming the joint power spectrum together with the attached phase,  $h_3(u, v) = \exp[i2\pi p_3(u, v)]$ , the detected image in the output plane is expressed by

$$o(x, y) = \text{FT}^{-1}\{\exp[i2\pi p_3(u, v)]\text{FT}\{\exp[i2\pi p_1(x, y)] + \exp[i2\pi p_2(x, y)]\}\}, \quad (2)$$

where FT and  $\text{FT}^{-1}$  denote the Fourier transform and the inverse Fourier transform, respectively. Both the functions  $p_1(x, y)$  and  $p_3(u, v)$  in the optical architecture are iteratively modified during the iteration process. Finally, the retrieved phases are obtained when the iterated image converges. That is, we can obtain an approximate image  $\hat{o}(x, y)$  in the output plane using two retrieved phases in the input plane and the attached phase mask, respectively.

The only difference from the conventional JTC is that an extra phase mask is attached to the SLM that is used to display the joint power spectrum of the input phase functions. With this attached phase-only information for the real power spectrum, the real part (magnitude)

of their Fourier transform can then be asymmetric. That is, an asymmetric image can be reconstructed in the output plane of this modified JTC architecture. Two phase functions,  $h_1(x, y)$  and  $h_3(u, v)$ , have to be retrieved in the proposed architecture. The multiple-phase-retrieval algorithm (MPRA) that can simultaneously retrieve two or more phase functions in a 4- $f$ -based optical architecture has been reported in Ref. [7]. Although the proposed architecture is different from the 4- $f$ -based architecture, the multiple phase retrieval algorithm can still be applied on the proposed architecture to retrieve two phase functions of different sizes.

To retrieve the phase functions based on a predefined target image  $f(x, y)$  and a random phase function  $h_2(x, y) = \exp[i2\pi p_2(x, y)]$ , the POCS algorithm incorporated with the MPRA is employed. During the iteration process, two constraints are used in the proposed scheme. First, the recovered image detected in the output plane should be forced to the predefined target image (the output plane constraint). That is, only the amplitude part in the detection plane is forced to be the target image. The phase part can be ignored. Second, the retrieved function in the input plane should be phase only (the input plane constraint). That is, the amplitude is forced to be unity.

The block diagram of applying the POCS and multiple phase retrieval algorithms on the proposed architecture is shown in Fig. 3. Basically, this block diagram consists of two parts: the forward and the backward operations, which are corresponding to the forward and the backward light propagations in the proposed architecture, respectively. The detailed steps for both operations are described as follows:

1. Randomly generate the initial phase values in  $p_1(x, y)$  and  $p_3(u, v)$  for the retrieved phase functions,  $h_{1,0}(x, y)$  and  $h_{3,0}(u, v)$ , and the values in  $p_2(x, y)$  for the fixed phase

function  $h_2(x, y)$ .

2. Suppose that the iteration process reaches  $k^{\text{th}}$  step, where  $k = 1, 2, 3, \dots$ . Consider the forward operation shown in the upper part of the figure. The interference pattern shown in the CCD plane is shown in Eq. (1).
3. The square-law operation denotes that the CCD detects the intensity  $O'_k(u, v)$  of the interference pattern, while the phase information  $\exp[i\phi_k(u, v)]$  is extracted and stored for the use in the backward operation.
4. The intensity signal is transmitted to an SLM, to which the phase mask  $h_{3,k}(u, v)$  is attached and then illuminated by a plane wave. Therefore, a complex function  $O_k(u, v) = O'_k(u, v) \exp[i2\pi p_{3,k}(u, v)]$  is generated.
5. The inverse Fourier transform of the complex function  $O_k(u, v)$  can be detected in the output plane, which is expressed by

$$o_k(x, y) = \text{FT}^{-1}\{O_k(u, v)\} = |o_k(x, y)| \exp[i\angle o_k(x, y)]. \quad (3)$$

6. The mean square error (MSE) between the target and the iterated images is calculated by

$$\text{MSE} = \frac{1}{M \times N} \sum_{x=1}^M \sum_{y=1}^N [o(x, y) - |o_k(x, y)|]^2, \quad (4)$$

where  $M \times N$  is the size of the image. If the MSE is less than a predefined threshold value, the iteration process stops and the retrieved phase becomes the phase key. Otherwise, the backward operation described in the following steps is employed to modify the retrieved phase.

7. The  $k^{\text{th}}$  iterated image (the amplitude part of the signal in the output plane) is modified according to the output-plane constraint and becomes the constrained image  $\hat{o}_k(x, y)$ .
8. Since the constrained image is asymmetric, its Fourier transform  $\hat{O}_k(u, v)$  should be a complex signal, in which the phase part is then assigned as the  $k^{\text{th}}$  phase function  $h_{3,k+1}(u, v)$ .
9. For this new phase function  $h_{3,k+1}(u, v)$  with the power spectrum, the Fourier transformed is performed again to examine whether the detected image has converged or not from measuring the MSE between them. If the MSE is less than a predefined threshold value, the iteration process stops and the retrieved phase becomes the phase key. Otherwise, the following steps will proceed.
10. The power spectrum obtained in the forward operation is real and non-negative. Therefore, to make a non-negative signal, the original signal should subtract the minimum amplitude signal. That is,

$$O_k'''(u, v) = \hat{O}_k''(u, v) - \min\{\hat{O}_k''(u, v)\}. \quad (5)$$

11. To reconstruct the signal arriving at the CCD detector, the square root operation is applied on the non-negative signal and then combined with the pre-stored phase information. That is,

$$\bar{O}_k(u, v) = [O_k'''(u, v)]^{\frac{1}{2}} \exp[i\phi_k(u, v)]. \quad (6)$$

12. With the inverse Fourier transform of  $\bar{O}_k(u, v)$  and applying the input plane constraint, the newly retrieved phase  $h_{1,k+1}(x, y)$  can be obtained.



13. Set  $k = k + 1$  for the next iteration process that starts from Step 2. The iteration steps will not stop until that the MSE value is less than the predefined threshold or the iteration number reaches a given number.

Compared with the conventional JTC architecture, one more phase mask is used to reconstruct the target image. Because the phase data increase a lot, the reconstructed image in the proposed architecture is expected to own better fidelity. However, the additional phase mask requires extra cost and may suffer the misalignment problem.

### 3 Simulation Results

In computer simulation, both the asymmetric and symmetric images are used to test the proposed method. The comparison with the conventional JTC architecture about the symmetric image is also performed. First of all, two asymmetric images of size  $128 \times 128$ , the Lena image and the binary letters (the former is grayscale and the latter is binary) shown in Fig. 4 are used to test the proposed method. The phase functions  $h_1(x, y)$  and  $h_2(x, y)$  in the input plane are of size  $100 \times 30$  and located in centers of the upper- and lower-half planes, respectively. On the other hand, the phase function  $h_3(u, v)$  is of size  $128 \times 128$  and assumed to be perfectly attached to the SLM.

Consider the simulation results obtained for the iteration number 200. Figure 5 shows that both the asymmetric images can be reconstructed based on the proposed architecture. Obviously, both the recovered images are of superior quality. On the hand, the MSE of the iterated image and the target image are also shown in Fig. 6(a) and 6(b). As shown in this figure, less MSE is achieved for the grayscale image. **For 8-bit grayscale (0–255) images, the desired pixel values are distributed in 256 gray levels. On the other**

hand, the desired pixel values are only 0 and 255 for the binary images, . In the proposed system, the reconstructed image in the output plane is grayscale rather than binary. Obviously, larger errors in reconstructing binary images are expected. Thus the mean value of the MSEs for grayscale images is much less than that for binary images.

For different initial phase distributions, the iteratively retrieved phase pairs,  $h_1(x, y)$  and  $h_3(u, v)$ , are also different. Therefore, only the phase pairs retrieved together in the same iteration process should recover the target image. Having only one phase key, or having two phase keys but not belonging to the same pair could fail to recover the target image. Even an illegal user acquires the target image in the output plane and reproduces two phase masks, the security system cannot be broken. This feature is demonstrated in the tables shown in Figs. 7 and 8. Four pairs of the phase masks,  $h_{1,i}(x, y)$  and  $h_{3,i}(u, v)$ ,  $i = 1, 2, \dots, 4$ , are retrieved by the iteration process for the same target image. Both tables demonstrate that only the correct phase pairs can recover the target image, as seen along the diagonal of each table. When the mismatched phase pairs are used, blurred images with much lower peak signal-to-noise ratio (PSNR) values are obtained. The PSNR of a detected image  $\hat{o}(x, y)$  is defined as

$$\text{PSNR} = 10 \log_{10} \frac{255^2}{\text{MSE}[o(x, y), \hat{o}(x, y)]} \quad \text{dB.} \quad (7)$$

The retrieved phase keys lead to the correctly recovered images with some variation on their PSNR values. To obtain better phase keys, the PSNR performance can be used as the convergence criterion of the iteration process. Therefore, higher PSNR values for the reconstructed images can be guaranteed.

The data amount of the phase function  $h_3(u, v)$  is much larger than that of the phase  $h_1(x, y)$ . Therefore, the phase function  $h_3(u, v)$  dominates the quality of the recovered image. According to the PSNR or MSE values of the recovered images, one can easily determine whether the input phase keys are correct or not. **As shown in Figs. 8 and 7, however, even the phase keys belong to different iterations, the off-diagonal result images that are obtained from using the mismatched phase keys still show significant meaning, especially for the Letter image. This demonstrates that the phase key attached at the SLM dominates the recovered image quality.** It could be a disadvantage of the proposed method because the recovered image may be visible when mismatched keys are used. However, the proposed system focuses on image verification rather than image encryption. To distinguish the keys are correct or mismatched pairs, the image quality represented by PSNR is measured. If one cannot recover the target image with good quality, at least one of the phase keys are incorrect and thus the user cannot pass the verification. According to the simulation result, we have shown that there is a big gap ( $> 6$  dB) for the PSNR values between the images recovered by the correct and incorrect phase keys. To further make improvement on the discrimination, a large threshold value 200 is used to binarize the pixel values of the output images shown in Fig. 7. Fig. 9 shows the results after the thresholding scheme is applied on the detected images shown in Fig. 7. Only the diagonal images are recognizable. Therefore, the discrimination between the diagonal and off-diagonal images can be greatly improved.

Consider the symmetric images, Lena and letters “EFLO,” shown in Figs. 10(a) and

11(a). Figures 10(b) and 11(b) show the simulation results for the recovered images from the proposed method, while Figs. 10(c) and 11(c) show the recovered images from the conventional JTC architecture. Obviously, the proposed method outperforms the conventional JTC architecture very much. On the other hand, the MSE measurements are also performed and shown in Fig. 12. For both the binary letters and the Lena images, the proposed method significantly decreases the MSE. From the simulation results for both the asymmetric and symmetric images, the proposed method greatly improves the image quality from the conventional JTC architecture.

**Consider the security level of the conventional and the proposed architectures. The sizes of the phase functions  $h_1(x, y)$  and  $h_3(u, v)$  are  $100 \times 30$  and  $128 \times 128$ , respectively. If the 8-bit phase resolution is employed, the numbers of the possible combinations of the phase keys in the conventional (only  $h_1(x, y)$  is employed) and the proposed (both  $h_1(x, y)$  and  $h_3(u, v)$  are employed) systems are  $256^{100 \times 30}$  and  $256^{100 \times 30 + 128 \times 128}$ , respectively. The latter number is large enough to thwart the brute-force attack. Compared with the conventional scheme, the attached phase function  $h_3(u, v)$  provides much more key space and thus much more security degree can be achieved in the proposed method.**

## 4 Conclusion

The security optical systems based on the conventional JTC architecture can only perform the symmetric-image verification because the magnitude of the Fourier transform of the real and non-negative joint power spectrum is symmetric. In this paper, we propose an optical architecture that can perform the asymmetric-image verification. The proposed

architecture basically is similar to the conventional JTC one except that an additional phase mask is attached to the SLM in the JTC architecture. Higher security is obtained in the proposed optical verification system because two phase keys are employed. From the simulation results, asymmetric images can be reconstructed with fine fidelity. For symmetric images, the proposed architecture can also yield the better image quality than the conventional JTC architecture.

## **5 Acknowledgment**

This research was partially supported by the National Science Council, Taiwan, under contract NSC 92-2213-E-224-047. In revising this work, the assistance from Mr. Chao-C. Chen is truly appreciated.

## References

- [1] T. Nomura and B. Javidi, “Optical encryption using a joint transform correlator architecture,” *Optical Engineering*, **39**(8), pp. 2031–2035 (2000)
- [2] D. Abookasis, O. Arazi, J. Rosen, and B. Javidi, “Security optical systems based on a joint transform correlator with significant output images,” *Optical Engineering*, **40**(8), pp. 1584–1589 (2001)
- [3] B. Javidi and J.L. Horner, “Optical pattern recognition for validation and security verification,” *Optical Engineering*, **33**(6), pp. 1752–1756 (1994)
- [4] J.-L. de Bougrenet de la Tocnaye, E. Que’mener, and G. Keryer, “Principle of pattern-signature synthesis and analysis based on double optical correlators,” *Applied Optics*, **39**(2), pp. 199-211 (2000)
- [5] J.R. Fienup, “Phase retrieval algorithm: a comparison,” *Applied Optics*, **22**(15) pp. 2758–2769 (1982)
- [6] J. Rosen, “Learning in correlators based on projection onto constraint sets,” *Optics Letters*, **18**, pp. 1183–1185 (1993)
- [7] Hsuan T. Chang, W.C. Lu, and C.J. Kuo, “Multiple-phase retrieval for optical security systems using random phase encoding,” *Applied Optics*, **41**(23), pp. 4825–4834 (2002)

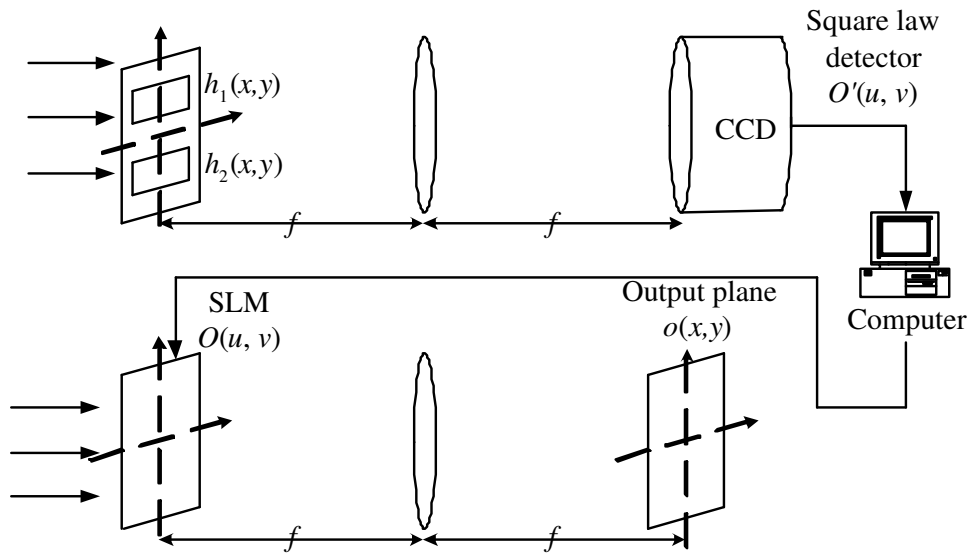


Figure 1: Optical setup of the conventional JTC architecture for image verification.

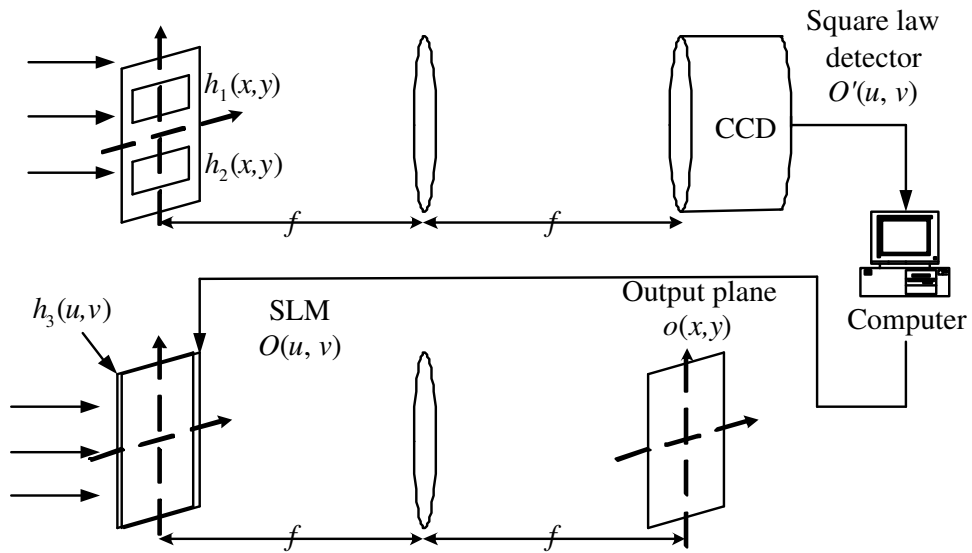


Figure 2: The optical setup of the proposed architecture. An extra phase mask  $h_3(u,v)$  is attached to the SLM to introduce the phase components to the joint power spectrum.

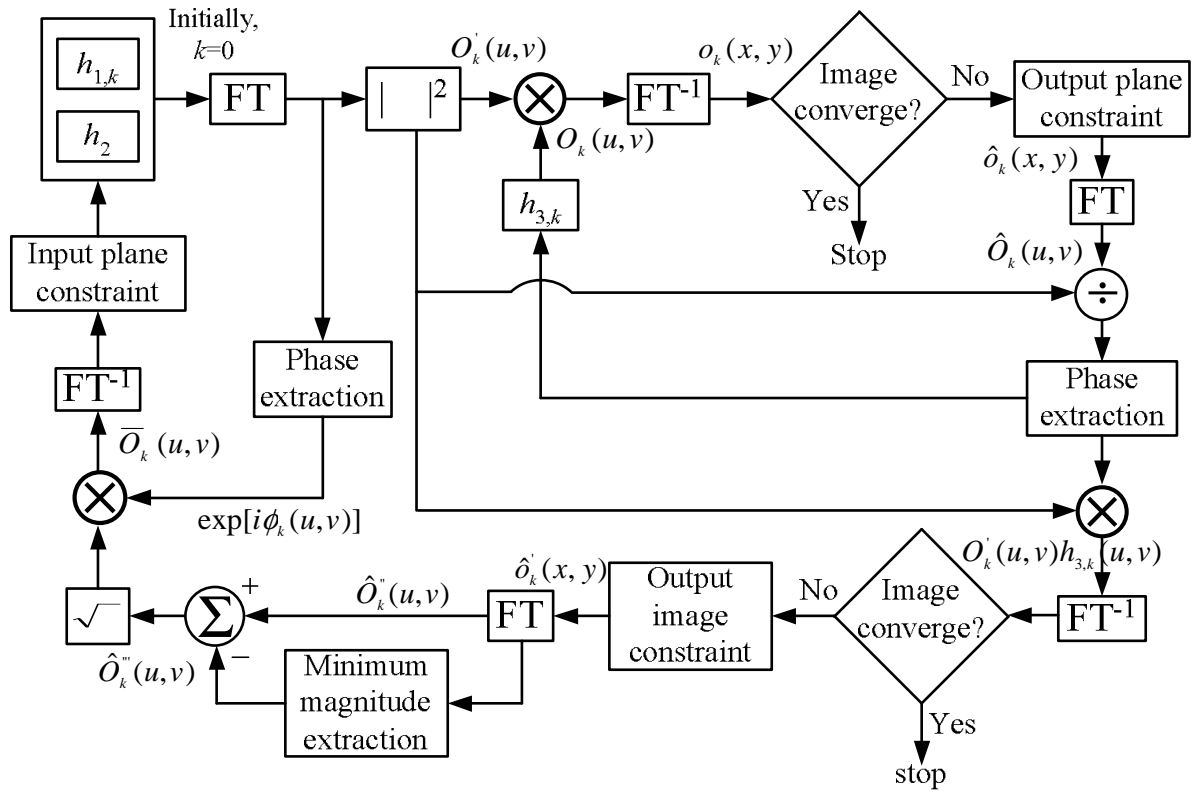
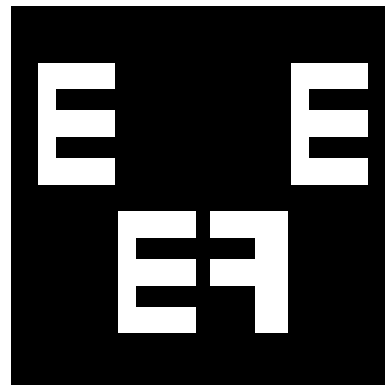


Figure 3: The block diagram of the proposed architecture.



(a)



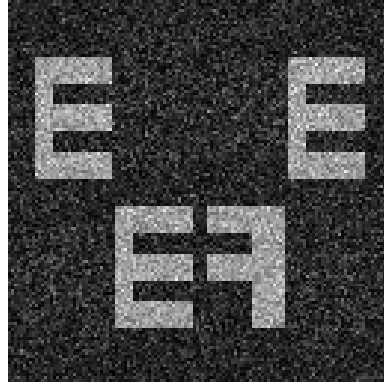
(b)

Figure 4: The test images: (a) Lena, (b) Letters.



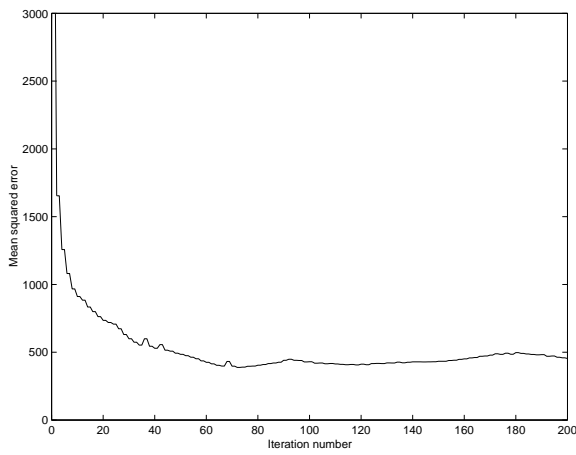


(a)

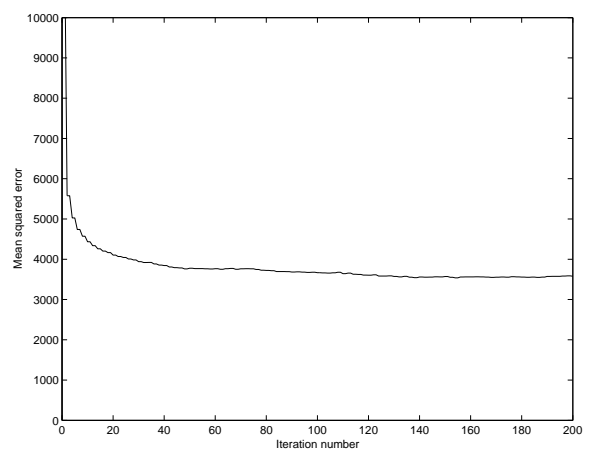


(b)

Figure 5: The images recovered from the proposed architecture: (a) Lena, (b) Letters.



(a)



(b)

Figure 6: The MSE results of the proposed architectures for: (a) Lena, (b) Letters.

	$h_{1,1}$	$h_{1,2}$	$h_{1,3}$	$h_{1,4}$
$h_{3,1}$				
PSNR	17.46 dB	11.21 dB	11.00 dB	11.17 dB
$h_{3,2}$				
PSNR	11.12 dB	17.57 dB	11.16 dB	11.07 dB
$h_{3,3}$				
PSNR	11.08 dB	11.20 dB	17.84 dB	11.12 dB
$h_{3,4}$				
PSNR	11.18 dB	11.16 dB	11.17 dB	17.66 dB

Figure 7: Simulation results for different phase pairs for the binary target image.


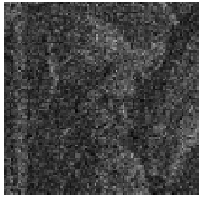
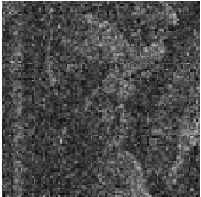
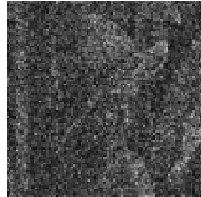
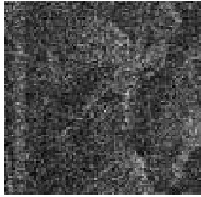

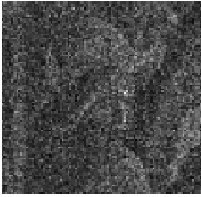
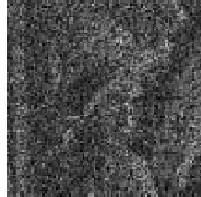
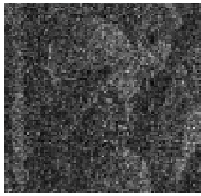
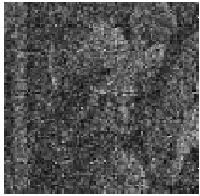

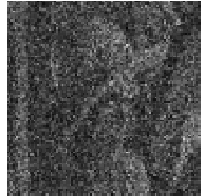
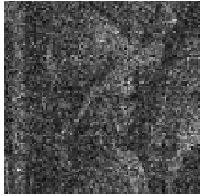
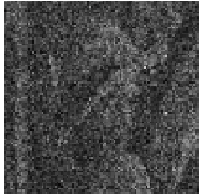
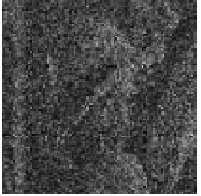

	$h_{1,1}$	$h_{1,2}$	$h_{1,3}$	$h_{1,4}$
$h_{3,1}$				
PSNR	20.89 dB	13.62 dB	13.72 dB	13.64 dB
$h_{3,2}$				
PSNR	13.61 dB	20.97 dB	13.62 dB	13.64 dB
$h_{3,3}$				
PSNR	13.63 dB	13.63 dB	20.87 dB	13.62 dB
$h_{3,4}$				
PSNR	13.60 dB	13.59 dB	13.63 dB	20.86 dB

Figure 8: Simulation results for different phase pairs for the grayscale target image.

	$h_{1,1}$	$h_{1,2}$	$h_{1,3}$	$h_{1,4}$
$h_{3,1}$				
$h_{3,2}$				
$h_{3,3}$				
$h_{3,4}$				

Figure 9: Simulation results after the thresholding scheme is applied on the detected images shown in Fig. 7.

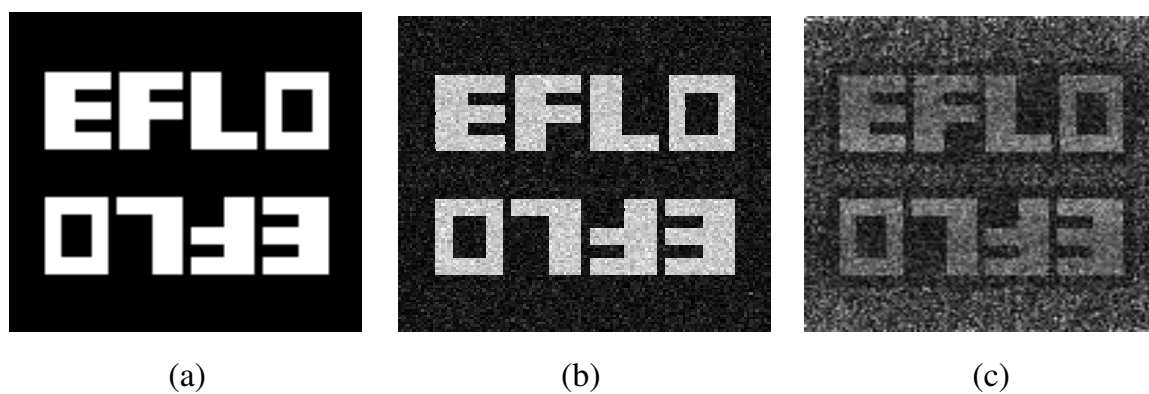


Figure 10: Simulation results for the symmetric binary image.

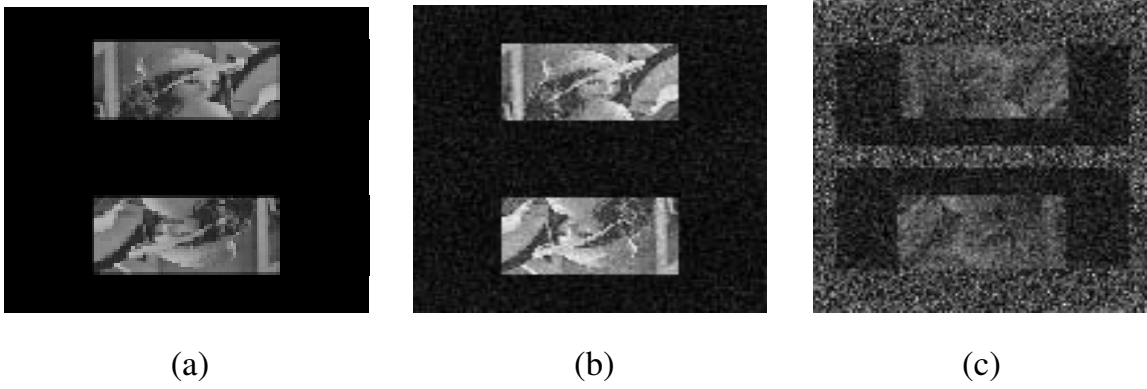


Figure 11: Simulation results for the symmetric grayscale image.

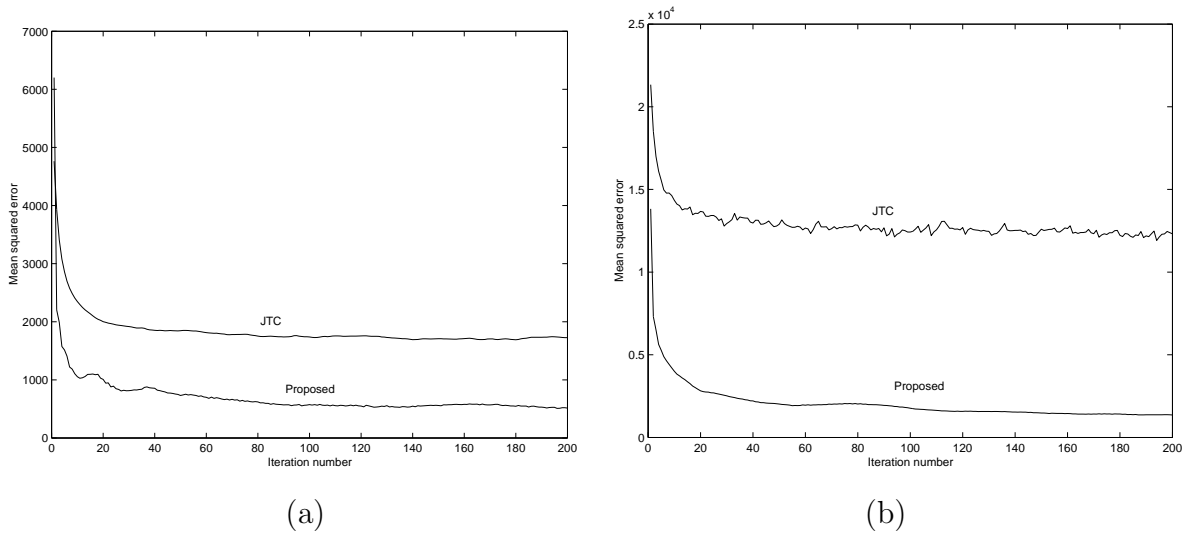


Figure 12: The MSE results of the proposed architectures for symmetric images: (a) Lena, (b) Letters.