CHIN. PHYS. LETT. Vol. 34, No. 11 (2017) 114204

Invisible Visual Cryptography *

Yi-Shi Shi(史祎诗)[1,2**], Xiu-Bo Yang(杨秀波)[1]

[1]College of Opto-Electronics, University of Chinese Academy of Sciences, Beijing 100049
[2]Academy of Opto-Electronics, Chinese Academy of Sciences, Beijing 100094

(Received 4 September 2017)

We propose to realize visual cryptography in an indirect way with the help of diffractive optics, the pure-amplitude keys being substituted with the phase-only keys that are invisible for common-used intensity detectors, leading to the significantly enhanced security and improved usability for practice. Three typical realizations are provided by using static or dynamic diffractive optical elements, and the new concept of invisible visual cryptography (IVC) may be established. This concept is demonstrated by a compact opto-electronic system with only one spatial light modulator within time-delayed exposure, maintaining the fast speed of decryption and no requirement to the calculation of decryption in conventional visual cryptography. Further, IVC shows the immunity to noises and good information capacity, which is partly inherited from diffractive optics. IVC might suggest a new strategy for visual cryptography with the respective of diverse realizations, such as opto-electronic or even bio-chemical or other methods.

PACS: 42.30.Kq, 42.30.Sy, 42.30.Va DOI: 10.1088/0256-307X/34/11/114204

Based on the Moiré effect from random dots, Glass found that the human visual system (HVS) can detect local correlations in the presence of noise, and combine local correlations from different regions of the visual field.[1] Kafria and Keren proposed that this ability of the HVS can be used to encrypt pictures and shapes by random grids.[2] Unfortunately, the work had not received sufficient attention until the concept and frame of visual cryptography (VC) were proposed and demonstrated mathematically by Naor and Shamir.[3] A general (k, n)-VC describes the k out of n secret sharing methods, in which a dealer provides a transparency to each one of the n users; any k of them can see the image by stacking their transparencies, but any $k-1$ of them gain no information about it. VC can decode encrypted images without any cryptographic computations. It is highly secure and very easy to implement. Recently, VC was improved gradually with the proposal of extended, colorful, dynamic properties, without pixel expanded VC.[4–9]

As we know, ciphertexts of VC are pure-amplitude and random-like binary images, which are easy to attract the attention of the attackers who then make the encryption of VC fail. To mitigate this problem, we propose invisible visual cryptography (IVC) to realize VC in an indirect way with the help of diffractive optics. We substitute the pure-amplitude keys, which are visually visible, with the phase-only keys which are actually invisible for the human eyes and intensity detectors. The transformation from the original pure-amplitude keys to the phase-only keys can be accomplished by a phase retrieval algorithm in the computer, and further, the phase-only keys can be realized with static or dynamic diffractive optical elements (DOEs), which allow a much safer way to achieve IVC. The optical diffraction of phase-only keys generates the expected wavefront distribution under a compact opto-electronic system, resulting in indirect realization of IVC. It maintains the fast speed, visualizability and simplicity of decryption in VC, meanwhile significantly improving security and usability for practice. In this work, we propose three typical schemes to attain IVC, and perform experiments to demonstrate its feasibility and reveal a series of properties, such as the robustness and the secret information capacity.

In principle, the core of IVC is the transformation between original pure-amplitude keys of VC and 'invisible' phase-only keys that are invisible for the human eye and the direct detection of common-used intensity detectors, such as the charge-coupled device (CCD). This invisibility of keys is the key reason why IVC has great security and concealment. IVC improves invisibility and security of VC from the standpoint of optics although basic security is guaranteed by VC.

In encryption, the transformation can be divided into two steps. The first step is to encode directly the message via general VC, in which the image plaintext is encoded to n pure-amplitude keys (subimages) according to the (k, n) VC. The second step is to transform encoded visible pure-amplitude keys to invisible phase-only keys. It is achieved by the phase retrieval algorithm in the computer. The phase distribution of the DOE can be obtained by applying the phase retrieval algorithm, such as the GS algorithm, reduce error algorithm and hybrid input-output algorithm.[10,11] The DOE can control the optical field distribution and the wavefront distribution to obtain an expected amplitude pattern by the optical diffraction. The phase distributions of DOEs are the phase-

*Supported by the National Natural Science Foundation of China under Grant No 61575197, the K. C. Wong Education Foundation, the Fusion Foundation of Research and Education of Chinese Academy of Sciences, and the Youth Innovation Promotion Association of Chinese Academy of Sciences under Grant No 2017489.

**Corresponding author. Email: optsys@gmail.com

© 2017 Chinese Physical Society and IOP Publishing Ltd

only keys of IVC in essence. The phase-only key can be represented in the form of the DOE or the digital phase distribution image. The invisibility of phase-only keys enhances the invisibility and security of IVC significantly. In experiment, DOE_1 and DOE_2, as shown in Fig. 1, are pictorial gray distributions of phase-only keys, which are based on the $(2, 2)$ VC. The gray levels of DOE_1 and DOE_2 between 0 and 1 are corresponding to phase values between 0 and 2π.

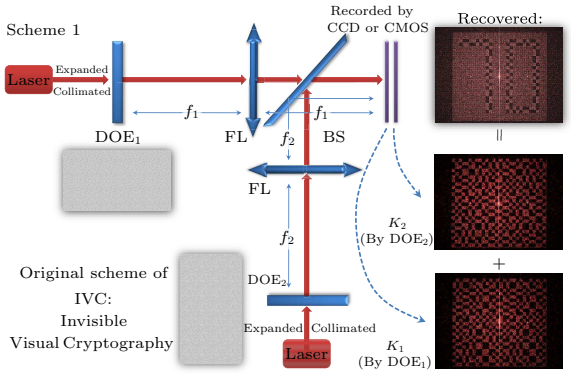


Fig. 1. Decryption schematic diagram of IVC. Laser and Fourier lens decrypt invisible phase-only keys of IVC (DOE_1, DOE_2) to amplitude diffraction patterns (K_1, K_2), respectively. Diffraction patterns are coupled and stacked by the beam splitter to obtain the encrypted message.

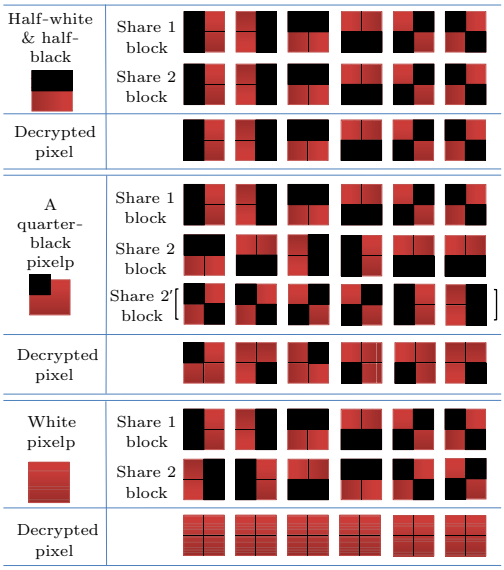


Fig. 2. Three possible results of stacking of share blocks in IVC. Decryption is realized by the incoherent stacking and the light reflection.

In decryption, the opto-electronic system transforms the invisible phase-only keys to amplitude patterns by the optical diffraction. Then transformed images are superimposed by optics element, other than the direct stacking of sub-images in VC. Figure 1 is a decryption schematic diagram of IVC based on the $(2, 2)$ VC. Firstly, the laser beam is shaped by the attenuator and beam expander after being emitted from the He-Ne laser. Then, the beam illuminates vertically on the phase-only key and does diffract. Next, the diffractive beam passes through the Fourier lens, and images on the back focal plane of the lens according to the scalar diffraction theory. Finally, all diffraction patterns are combined and superimposed by a special optics element, such as the beam splitter. They are stacked by this way. In Fig. 1, K_1 and K_2 are decrypted amplitude patterns from phase-only keys DOE_1 and DOE_2, respectively. They are corresponding to original pure-amplitude keys of the $(2, 2)$ VC. The recovered image shows the combined image by the beam splitter. The message, that is the numbers of 70, can be recognized clearly.

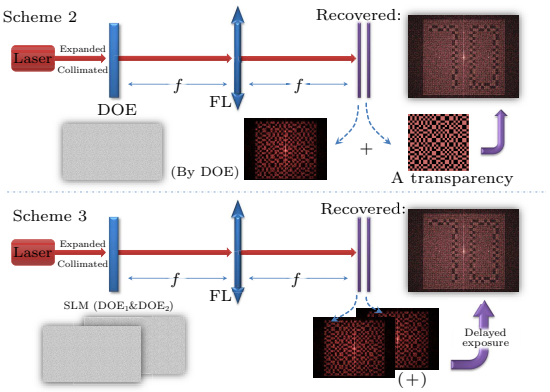


Fig. 3. Two equivalent realization schemes of IVC. Decryption is realized by a single-path opto-electronic system. Diversified keys (scheme 2) and SLM (scheme 3) realize flexibly the IVC.

IVC has some differences from VC in the share block. IVC decrypts the message via the light reflection, but VC utilizes the light transmission, despite the fact that they ended up with incoherent stacking. We define light pixel and black pixel to logical 1 and 0, respectively. In decryption, addition of 0 and 1 is 1 in IVC, but the result is 0 in VC. That is, the stacking of sub-images in VC follows logical AND, while the superimposition of diffraction patterns in IVC follows logical OR. Figure 2 shows three possible results of stacking of different share blocks based on the $(2, 2)$ VC in decryption. A share block is comprised of four pixels arranged in a 2×2 array, in which 2 pixels are light, and the other 2 pixels are dark. In practice, the arrangement of pixels and the number of light pixels are adjustable. As shown in the first row of Fig. 2, if pixels of two share blocks are the same, the stacking is a half-red (laser light) and half-black expanding pixel. The third row shows that if pixels of two share blocks are just the reverse, the stacking of shares will be a pure red expanding pixel. In the second row, if one pair of pixels of two share blocks is black, but the other pairs of pixels are different, the expanding pixel will be quarter-black pixel. Meanwhile, the stacking of share 2 block and share 1 block is equal to the stacking of share $2'$ block and share 1 block, and it shows that the same expanding pixel can be attained by stacking of different shares. What is more, this principle of share block, as shown in Fig. 2, is efficient to the extended IVC based on the (k, n) VC.

The idea of IVC can be realized by diverse and flexible implement methods other than VC. We take two schemes, as shown in Fig. 3, as examples to explain this diversity in detail. The scheme 2 of Fig. 3 adopts diverse key forms and simpler linear single-path optics system instead of coupling system of Fig. 1. It just needs one laser and one Fourier lens. In encryption, pure-amplitude keys that are part of subimages from VC and phase-only keys generated from the other part of subimages make up all ciphertexts of IVC. Compared with the scheme 1 in Fig. 1, phase-only keys and pure-amplitude keys group into a huge key space, leading to enhanced security and flexibility. When decrypting ciphertexts, phase-only keys are decrypted by the single-path optics system and optics diffraction. Diffraction patterns image and superimpose directly on the pure-amplitude keys that are printed on opaque plane, to obtain the recognizable decrypted image.

Both static and dynamic IVCs can be realized conveniently by scheme 3 of Fig. 3, in which all ciphertexts are directly generated by corresponding phase-only keys. In the single-path optics system of decryption, a phase-only spatial light modulator (SLM) simulates and replaces phase-only keys, and decrypted diffraction patterns are received by an image detector. In the static scheme, phase-only keys are separately uploaded to the SLM and then decrypted by optical diffraction. Finally, all received diffraction patterns are added in pixel-to-pixel to obtain the decrypted image. However, in dynamic realization, all phase-only keys are uploaded simultaneously to the SLM in alternative displayed dynamic image, and then decrypted continuously via optics diffraction. Finally, image detector receives diffraction patterns and stacks directly them by the delayed-time exposure to obtain the final decrypted image. Compact opto-electronic deceive and diversified decryption methods make IVC have great flexibility and application.

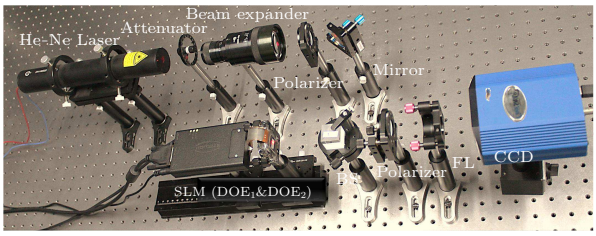


Fig. 4. Single-path opto-electronic decryption deceit of IVC. The scheme 3 of Fig. 3 is adopted. SLM simulates and replaces phase-only keys in decryption. Improved laser beam illuminates vertically on SLM, and reflected beam is imaged on the CCD by the Fourier lens.

We utilize the single-path opto-electronic decryption device as shown in Fig. 4 to research IVC. The scheme 3 of Fig. 3 is adopted to research for flexibly developing advantages of the opto-electronic system in compactness, simplicity and stability. Phase-only keys are generated by encryption computation in computer. In Fig. 4, the laser beam is emitted from the He-Ne laser, and the attenuator and beam expander are placed on the downstream of laser. Then, the laser beam is reflected vertically to the liquid crystal display of SLM by a mirror and a beam splitter after being polarized by a polarizer (HOLOEYE PLUTO reflex phase-only SLM, the spatial resolution of the liquid crystal display is 1920×1080 pixels, and single pixel pitch is $8\,\mu$m, and phase level has 8 bits and 256 gray levels). The liquid crystal display of the SLM simulates the phase distribution of DOE to represent the phase-only key of IVC. When the laser beam passes through it, the SLM modulates the laser beam and changes optical field distribution. After that, the laser beam, reflected from the SLM, passes through the beam splitter and meets diffraction. Next, a polarizer is used as an analyzer to detect polarization of the laser beam. Finally, the diffraction laser beam images on the far field. The function of the Fourier lens is to move the diffraction pattern from far field to near field. The CCD camera receives the diffraction pattern at the back focal plane of the lens (the image detector is the Coolsnap EZ CCD, whose signal pixel pitch is $6.45\,\mu$m, size of receiving area is 1392×1040 pixels. Its exposure time is adjustable). In experiment, if keys are decrypted one-by-one, and received diffraction patterns are added in pixel-by-pixel, the decryption is static. When all keys are uploaded to the SLM via the time-sharing, the above single-path opto-electronic system can realize flexibly dynamic decryption via time-delayed exposure of the camera. In addition, just only the camera is required to be placed at the back focal plane of the lens, but the phase-only keys are not strictly required to be set at the front focal plane of the lens.

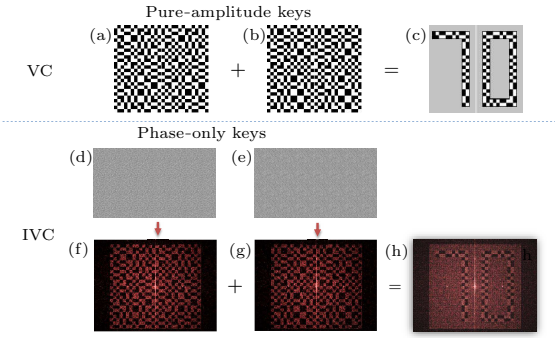


Fig. 5. Experimental results of IVC based on the $(2, 2)$ VC. Here (a) and (b) are ciphertexts of the numbers 70 under the $(2, 2)$ VC, and their stacking is decrypted image (C) in VC; (d) and (e) are phase keys of IVC; (f) and (g) are received diffraction images from decryption by the opto-electronic system; and (h) is the addition of (f) and (g), which is the decrypted image of IVC.

The experimental results are shown here. The feasibility of IVC is verified strongly by the experimental results, as shown in Fig. 5. The verified experiment adopts scheme 3 as shown in Fig. 3. When encrypting numbers 70, firstly, an algorithm of the $(2, 2)$ VC encodes the image with numbers to pure-amplitude subimages (keys). Figures 5(a) and 5(b) are the encoded pure-amplitude subimages of VC. If

the subimages of VC are printed on transparencies and stacked together accurately, Fig. 5(c) will be their decrypted image. We utilize the matching software of the SLM which is based on the phase retrieval algorithm to transform pure-amplitude keys to phase-only keys. This software requires subimages not exceeding 200×200 pixels. The transformed results, as shown in Figs. 5(d) and 5(e), are phase-only keys of IVC, and the phase distributions of DOEs can also be denoted by them. In Fig. 5, invisible phase distributions are denoted by different gray levels.

Decryption is verified by the static realization of scheme 3 in Fig. 3 by the help of the single-path optoelectronic decryption deceit as shown in Fig. 4. Firstly, phase-only keys (Figs. 5(d) and 5(e)) are separately uploaded to the SLM of the decryption deceit and decrypted. Decrypted diffraction patterns are received from the camera as shown in Figs. 5(f) and 5(g). The result shows that diffraction patterns are quite corresponding to pure-amplitude subimages of VC. Then, diffraction patterns are added in pixel-by-pixel to obtain the final decrypted image of IVC as shown in Fig. 5(h). The results show that numbers 70 can be clearly recognized, although there is some noise. The above experimental results demonstrate the validity of the proposed method.

A dynamic scheme achieved by time-delayed exposure of the CCD can intuitively and real-timely realize IVC in a flexible way. As we know, incident rays within an exposure time of the camera can be imaged on the same image in superimposing. This feature is utilized to realize the dynamic scheme of IVC. In this scheme, all ciphertexts are phase-only keys as shown in Figs. 5(d) and 5(e), and decryption deceits as shown in Fig. 4. In decryption, all phase-only keys are processed to an alternative displayed dynamic image with frequency of 50 Hz and then uploaded to the SLM. Next, we extend the exposure time of the camera until receiving a clear and stable diffraction pattern. Following with the extension of exposure time, the decrypted image is from disordered to fuzzier, finally to clarity. The definition and identifiability are gradually rising. However, the exposure time is greater than 0.25 s, the decrypted image is ideal. The above result shows that the dynamic scheme of IVC is feasible.

We introduced the correlation coefficient (Co) to help the comprehension of the decrypted result of the dynamic IVC. The value of Co between two images A and B is defined as follows:

$$Co(\mathrm{A},\mathrm{B}) = cov(\mathrm{A},\mathrm{B})(\sigma_{\mathrm{A}}\sigma_{\mathrm{B}})^{-1}, \tag{1}$$

where $cov(\mathrm{A},\mathrm{B})$ is the cross-covariance between A and B, and σ is the standard deviation. Here Co denotes the similarity of both images in mathematics. Images A and B are correspondingly decrypted images of static and dynamic realizations in IVC. The relationship between Co and the exposure time is shown in Fig. 6. This figure shows that Co is increased overall, and definition of decrypted image is raised markedly, with the extension of the exposure time. When the exposure time rises to 0.25 s, the decrypted image is ideal.

Strong robustness is shown by testing in IVC. It brings about great stability in practical applications. In the test, the random noise with great irregularity and interference ability is used to evaluate the robustness for convincing. All kinds of noises are focused on the most vulnerable phase-only keys in random noise. Firstly, we multiply the random noise by the number X, which is defined to intensity coefficient. Then phase-only keys are added by random noises with different X, to simulate noise-polluted keys. Finally, polluted keys are decrypted via the static realization method of IVC. The definition of decrypted image is served as the criterion to evaluate the quality of decryption. Meanwhile, Co between decryption images from polluted and non-polluted phase-only keys is calculated to analyze quantitatively the robustness.

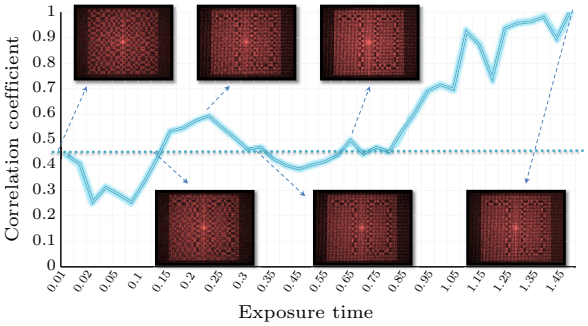


Fig. 6. Image of relationship between Co and exposure time in dynamic scheme, and some critical decrypted images. When the exposure time is larger than 0.25 s, ideal decrypted image will be achieved.

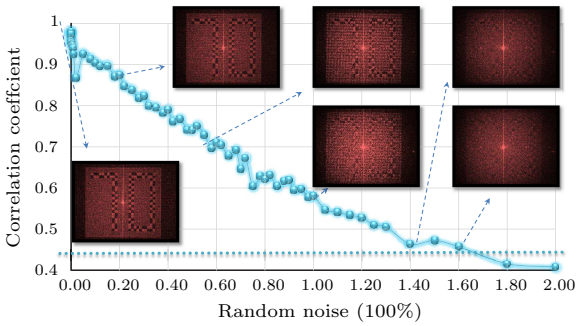


Fig. 7. Diagram of relationship between Co and X, and decrypted images of several representative X. The value of Co and definition of decrypted image are gradually declined as X increases. When X is not larger than 0.6, the decrypted image will be recognizable and acceptable.

To explore the maximum of the information capacity of image in each encryption, we use the method of IVC to handle images generated by joining multiple images of digits 0–9. Digits images are arranged in $a \times b$, and the size of them is 85×157 pixels. When the decrypted image can be recognized clearly, the maximum quantity of digits is defined to the maximum of the information capacity in IVC. For simplicity, Co is not analyzed. In actual experiment, we test the images that digit images are arranged in 2×1, 4×2, 6×3

and 8×4. The decrypted results, as shown in Fig. 8, indicates that the decrypted image with 6×3 digits can be recognized clearly although there is zero-order diffraction, but the image with 8×4 digits is unrecognizable. Thus the maximum of the information capacity is 6×3, namely 18 digits. This exploration shows that IVC has great information capacity although the pixel expansion of VC and diffraction effects decrease the identifiability. It must be pointed out that information capacity is not a standard value, but reference under the condition of this experiment. All experimental apparatus and methods, such as the SLM, the CCD camera, and phase retrieval algorithm, can affect the test results. High-precision experimental apparatus will make the maximum information capacity increase in a certain extent.

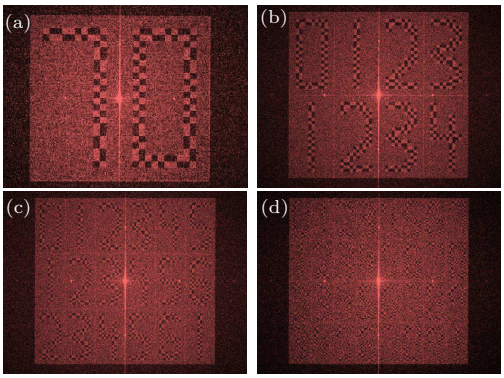


Fig. 8. Results of information capacity test. (a)–(d) The decrypted images from the images with the number of digits being 2×1, 4×2, 6×3 and 8×4, respectively. Digits of (c) are recognizable, but digits of (d) are not ideal.

In conclusion, we have proposed a new kind of realization approach for VC. It remedies the invisibility defect of VC, and can be flexibly achieved via diverse methods. The phase retrieval algorithm transforms pure-amplitude keys produced by general VC to invisible phase-only keys. The opto-electronic system and the optics diffraction realize the decryption from phase-only keys to original image in the static or dynamic method. The experimental results demonstrate feasibility and robustness of the proposed method. IVC mitigates greatly the invisibility, and enhances significantly the security and application of VC. It might inspire a new idea that combines multiple techniques[12,13] to enhance the security and application of VC.

References

[1] Glass L 1969 *Nature* **223** 578
[2] Kafri O and Keren E 1987 *Opt. Lett.* **12** 377
[3] Naor M and Shamir A 1995 *Lecture Notes in Computer Science* **950** 1
[4] Ateniese G, Blundo C, Santis A D and Stinson D R 1996 *Inf. Comput.* **129** 86
[5] Hou Y C 2003 *Pattern Recognit.* **36** 1619
[6] Yamamoto H, Hayasaki Y and Nishida N 2004 *Opt. Express* **12** 1258
[7] Shyu S J, Huang S Y, Lee Y K, Wang R Z and Chen K 2007 *Pattern Recognit.* **40** 3633
[8] Machizaud J, Chavel P and Fournel T 2011 *Opt. Express* **19** 022709
[9] Machizaud J and Fournel T 2012 *Opt. Express* **20** 22847
[10] Gerchberg R W and Saxton W O 1972 *Optik* **35** 237
[11] Fienup J R 1982 *Appl. Opt.* **21** 2758
[12] Liu S T, Mi Q L and Zhu B H 2001 *Opt. Lett.* **26** 1242
[13] Liu Z J, Ahmad M A and Liu S T 2008 *Opt. Commun.* **281** 5322