ADVANCED QUANTUM TECHNOLOGIES
www.advquantumtech.com

Compressed 3D Image Information and Communication Security

Chengshuai Yang, Yuyang Ding, Jinyang Liang, Fengyan Cao, Dalong Qi, Tianqing Jia, Zhenrong Sun, Shian Zhang, Wei Chen,* Zhenqiang Yin, Shuang Wang, Zhengfu Han, Guangcan Guo, and Lihong V. Wang*

Ensuring information and communication security in military messages, government instructions, scientific experiments, as well as in personal data processing, is critical. In this study, a new hybrid classical–quantum cryptographic scheme to protect image information and communication security is developed by combining a quantum key distribution (QKD) and compressed sensing (CS). This method employs a QKD system to generate true random codes among the remote legitimate users and utilizes these random codes to encrypt and decrypt compressed 3D image information based on the CS algorithm. Therefore, this new technique can provide computational security in the image information transmission process by the encryption and decryption of CS algorithm, and the information and communication security can be evaluated in real time by monitoring the QKD system. Furthermore, this technique can directly transmit and reconstruct the compressed 3D image information based on the modified TwIST algorithm, and thus fewer random codes are required in QKD system, which can improve the information transmission bandwidth. Consequently, this technique not only provides a new application of a QKD system but also extends the CS-based image reconstruction from 2D to 3D. This study may open a new opportunity in the field of information and security communication.

1. Introduction

The protection of information and communication security is critical for the secret document transmission or important private communications, which may be related to national security, enterprise operation, or personal reputation. Therefore, the information and communication security technology has become the primary support research direction of governments in recent years. With the advent of super computers or future quantum computers, the computing or attack capacity is significantly improved. So, the information and communication security suffers from unprecedented threats. Several traditional public-key cryptography (PKC) methods, such as ECC, RSA, DSA, AES, and D-H, are vulnerable to attack.[1] Recently, several information and communication security technologies, which are based on novel encryption algorithm or quantum cryptography, have been developed to resist super or quantum computer attacks.[2] For example, quantum key distribution (QKD) uses the quantum mechanics to guarantee secure communication; it enables two parties to produce a shared random secret key known only to them, which can then be used to encrypt and decrypt messages[3–6]; quantum machine learning is an interdisciplinary of quantum physics and machine learning, its goal is developing the quantum algorithms that learn

C. Yang, F. Cao, Dr. D. Qi, Prof. T. Jia, Prof. Z. Sun, Prof. S. Zhang
State Key Laboratory of Precision Spectroscopy
East China Normal University
Shanghai, 200062, P. R. China
E-mail: sazhang@phy.ecnu.edu.cn

Y. Ding, Prof. W. Chen, Prof. Z. Yin, Prof. S. Wang, Prof. Z. Han, Prof. G. Guo
CAS Key Laboratory of Quantum Information
University of Science and Technology of China
Hefei, 230026, P. R. China
E-mail: weich@ustc.edu.cn

Y. Ding, Prof. W. Chen, Prof. Z. Yin, Prof. S. Wang, Prof. Z. Han, Prof. G. Guo
Synergetic Innovation Center of Quantum Information and Quantum Physics
University of Science and Technology of China
Hefei, 230026, P. R. China

Dr. J. Liang
Centre Énergie Matériaux Télécommunications
Institut national de la recherche scientifique
Université du Québec
Québec, J3 × 1S2, Canada

Prof. S. Zhang
Collaborative Innovation Center of Extreme Optics
Shanxi University
Taiyuan, 030006, P. R. China

Prof. L. V. Wang
Andrew and Peggy Cherng Department of Medical Engineering
Department of Electrical Engineering
Division of Engineering and Applied Science
California Institute of Technology
Pasadena, CA 91125, USA

DOI: 10.1002/qute.201800034

from data in order to improve existing methods in machine learning[7,8]; blind quantum computation is a quantum computation model, which can release the client who does not have enough abundant knowledge and sophisticated technology to perform the universal quantum computation[9,10]; quantum secure direct communication is to transmit the legitimate parties' secret message directly and securely in a quantum channel without creating a private key to encrypt and decrypt the messages.[11]

Previous studies have demonstrated that the hybrid classical-quantum cryptographic technique can provide a very useful strategy to protect the information and communication security.[12–19] For example, the QKD combined with a one-time pad (OTP) scheme has been demonstrated to be theoretically information-secure against an arbitrary computer attack.[12,13] However, this technique requires a large number of quantum keys, and the low key generation rate of QKD system significantly limits the key transmission distance due to the losses of photons in the optical fiber and low working efficiency of a single-photon detector. Thus, the key transmission distance can only reach hundreds of kilometers.[14–16] The post-quantum cryptography scheme,[17] which is based on coding theory, lattice theory, multivariate polynomials, and hash cryptosystems, achieves better performance than the prequantum scheme. However, the message, key, and signature sizes are usually very large, and this technique cannot resist the attack of all possible quantum algorithms. The hybrid scheme by combining QKD with other classical cryptography tools,[18,19] which employs the quantum-safe key and non-quantum-safe primitives, is considered to be a suitable information security protection technique. This technique can only provide short-term security, and the classical master key needs to be frequently updated. Obviously, these schemes can provide information and communication security protection, but several technical limitations to the practical applications are observed.

To overcome several limitations of previous classical-quantum cryptographic methods, here we present a new cryptographic scheme to realize the information and communication security by combining the QKD system and compressed sensing (CS) algorithm. The CS algorithm has been demonstrated to be a well-established tool for encoding and decoding the image information based on the image sparsity,[20–33] and therefore was considered to be a potential information and communication security technology. However, the key in the classical cryptographic method, which is generated by a computer, comprises the pseudo-random codes, and so the key may be vulnerable to an eavesdropper's attack. In our scheme, we utilize the true random codes (i.e., quantum key) that are generated by the QKD system to encode all 3D images and compress these encoded 3D images to a new 2D image, and finally employ the CS algorithm to reconstruct the original 3D images based on the measured 2D image and quantum key. We use one key to encrypt and decrypt the compressed 3D image information directly, which differs from previous methods,[20–24] in which one 2D image information transmission requires one key. Therefore, an important advantage of our scheme is that fewer random codes are required, which is highly useful for increasing the information transmission bandwidth. Using the true random codes as the key to encrypt and decrypt the compressed 3D images can provide the computational security of image information transmission, and the information and communication security can be evaluated in real time by monitoring the QKD system. In addition, the 3D image reconstruction based on the CS algorithm has robustness and security, which is beneficial to the improvement of the key generation rate in the QKD system by removing the post-processing procedure, such as error correction or privacy amplification.

2. Experimental Section

In our experiment, the entire experimental arrangement is shown in **Figure 1**. As shown in Figure 1A, the random binary codes are generated by the QKD system, which constitutes the quantum key, and the quantum key is transmitted by the quantum channel with the optical fiber, whereas the plaintext (i.e., image information) is encoded by using the quantum key, and the formed ciphertext is transmitted by the classical channel based on the Internet with the optical fiber. In the previous image encryption by the CS algorithm, the key generated by the computer includes pseudo-random codes,[10–14] but here the QKD system can provide the true random codes for the CS algorithm. We utilize a Faraday–Michelson QKD system that is based on phase encoding to generate the quantum key,[34,35] as shown in Figure 1B. In the transmitter Alice, a quantum laser (Q-laser) with the repetition rate of 1GHz generates the pulse train at the wavelength of 1550.92 nm. The intensity modulator (IM) is employed to prepare the decoy states, and then these pulses enter into the Faraday–Michelson interferometer (FMI) and are modulated to be the four BB84 phase states by phase modulator (PM). Before entering into the dense wavelength division multiplexing (DWDM), the pulses are attenuated into the single-photon lever using an attenuator (Att). The average photon number per pulse is 0.65 for the signal states while it is 0.01 for the decoy states, and the vacuum states are generated by non-triggering Q-laser. The three-port optical circulator (CIR) and a monitor (Mt) are used to prevent and detect possible Trojan-horse attack from the channel. The sync laser (S-Laser) can generate the sync light signal at the wavelength of 1549.32 nm, which will be attenuated and combined into the DWDM. In receiver Bob, the sync pulses are detected by an avalanche photodiode (APD) to keep Alice and Bob in sync. The BB84 phase-encoded pulses are decoded by the FMI on the Bob side, and then detected by single photon detectors (SPD). The average detection efficiency is about 20%, and the afterpulse probability and the total dark counts are less than 1.1% and 2×10^{-6} per gate, respectively. By the communication in the classical channel, Alice and Bob compare their basis, and the sifted keys with the same basis are reserved. When the error correction using low density parity check code and the privacy using universal hash functions is sequentially performed on the sifted keys, the final secure keys can be generated. To ensure the key correctness and security in the transmission process, we perform the error correction (EC) and privacy amplification (PA) in the post-processing procedure. The length of optical fiber is 25 km, and the clocking rate is 1 GHz at the sender, whereas the secure key generation rate is approximately 0.37 Mbps at the receiver due to various losses in the transmission process including the optical fiber and single-photon detector.

The encryption and decryption processes of 3D image information are shown in **Figure 2**. In the image encryption process, as shown in Figure 2A, these original images ($X(i)$) are

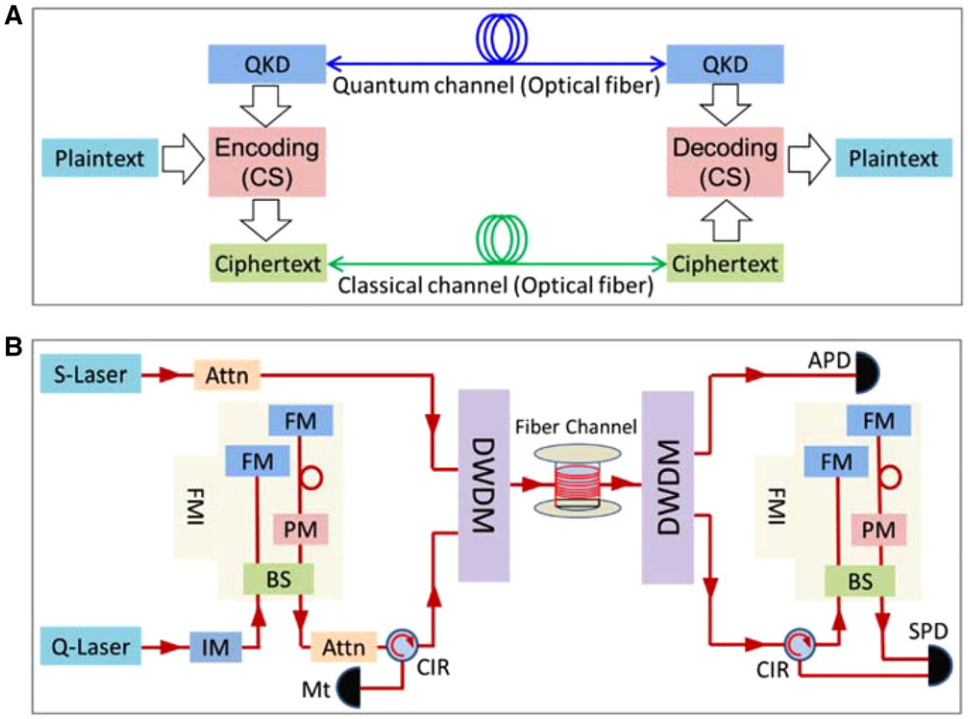

Figure 1. A) Schematic diagram of experimental setup for the compressed 3D image information secure communication. Here, the quantum key generated by the QKD system is transmitted by the quantum channel, whereas the ciphertext encoded by the compressed sensing (CS) algorithm is transmitted by the classical channel. B) The encryption key generation by the Faraday–Michelson QKD system, where Q-Laser, quantum laser; S-Laser, sync laser; Att, attenuator; IM, intensity modulator; FMI, Faraday–Michelson interferometer; PM, phase modulator; FM, Faraday mirror; BS, beam splitter; Mt, monitor; CIR, optical circulator; DWDM, dense wavelength division multiplexing; APD, avalanche photodiode; SPD, single photon photodiode.

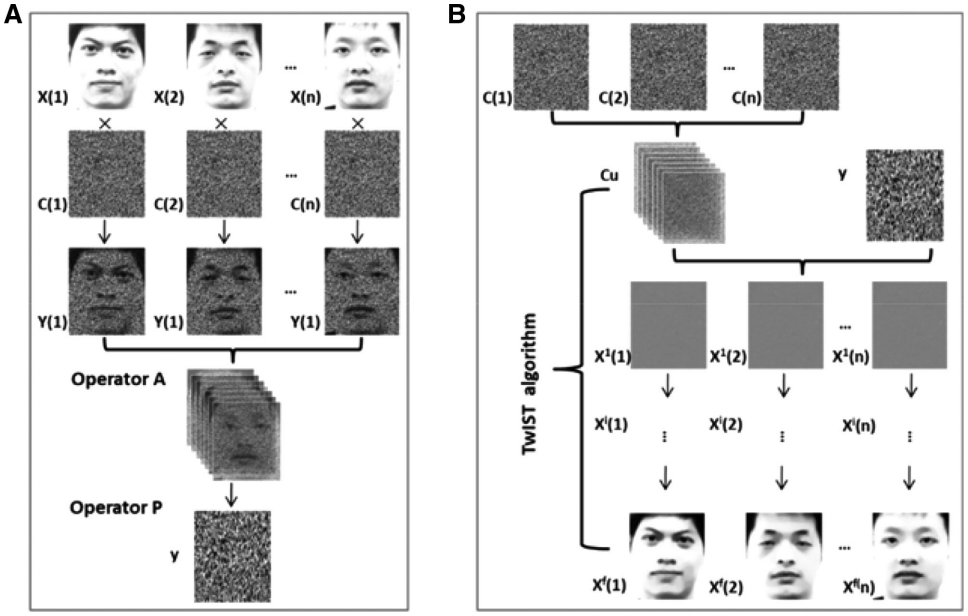

Figure 2. A) Encryption and B) decryption processes for the 3D image information based on the compressed sensing (CS) algorithm. In the encryption process, all the original images ($X(1)$, $X(2)$, …, $X(n)$) are encrypted by the same encryption key ($C(1)$, $C(2)$, …, $C(n)$), and compressed to one new image (y) by superimposing these encrypted images. In the decryption process, the compressed and encrypted image (y) is decrypted by a two-step iterative shrinkage/thresholding (TwIST) algorithm based on the superimposition key (Cu) and measurement image y.

encoded by the key ($C(i)$). Next, these encoded images ($Y(i)$) are superimposed in sequence, where each image is shifted by a pixel in the space along the vertical direction relative to the previous image. All encoded images are projected on one plane and form a new 2D encoded image (γ). In mathematics, the encryption process can be formulated as

$$\gamma = KX = PACX \tag{1}$$

where K is the image encryption operator, P is the projection operator, A is the superposition and shift operator, and C is the encoding operator. We employ the same codes (i.e., a quantum key) to encrypt all original images, and therefore the quantum key utilization is significantly improved, that is, this encryption method requires fewer random codes, which differs from the previous QKD that combines an OTP scheme.[2,3] In the image decryption process, as shown in Figure 2B, these same keys at the receiver are superimposed and projected on the space, and obtain a new key (Cu), which is similar to the encoded image superimposition in the encryption process. These original images can be reconstructed by using a CS algorithm (i.e., two-step iterative shrinkage/thresholding (TwIST)[34]) based on the new key (Cu) and the measurement image (γ). To reconstruct these images, Equation (1) must be solved in reverse. One way is to look for the minimal value of the following object function, and is given by[36]

$$f = \arg\min\left\{\tfrac{1}{2}\|\gamma - KX\| + \beta\phi(X)\right\} \tag{2}$$

where $\|\bullet\|$ is a l_2 norm of matrix, β is the regularization parameter, and $\phi(X)$ is the regularization function, which is written as[37]

$$\begin{aligned}\phi(X) = &\sum_{k=1}^{N_z}\sum_{i=1}^{N_x\times N_y}\sqrt{\left(\Delta_i^h X_k\right)^2 + \left(\Delta_i^v X_k\right)^2} \\ &+ \sum_{m=1}^{N_y}\sum_{i=1}^{N_x\times N_z}\sqrt{\left(\Delta_i^h X_m\right)^2 + \left(\Delta_i^v X_m\right)^2} \\ &+ \sum_{n=1}^{N_x}\sum_{i=1}^{N_y\times N_z}\sqrt{\left(\Delta_i^h X_n\right)^2 + \left(\Delta_i^v X_n\right)^2}\end{aligned} \tag{3}$$

where N_x and N_y are the row and column pixel numbers in each image, respectively; N_z is the image number; m, n, and k are the three indices; X_k, X_m, and X_n represent the 2D datum along the three indices k, m, and n, respectively; and $\Delta_i{}^h$ and $\Delta_i{}^v$ are the horizontal and vertical first-order local difference operators, respectively, on the 2D datum. In Equation (2), the minimization of the first term $\|\gamma\text{-}KX\|$ is used to obtain the maximal matching between the estimated measurement KX and the actual measurement γ, whereas the minimization of the second term $\beta\phi(X)$ is used to encourage X to be piecewise constant, where the regularization parameter β controls the relative weight of the two terms and obtains the almost identical physical reality. The iteration calculation in the image reconstruction is presented as follows:

$$X^1 = \Gamma_\lambda\left(X^0\right) \tag{4}$$

and

$$X^{i+1} = (1-\eta)X^{i-1} + (\eta-\xi)X^i + \xi\Gamma_\lambda\left(X^i\right) \tag{5}$$

for $i \geq 1$, Γ_λ can be defined as

$$\Gamma_\lambda(X) = \Phi_\lambda\left(X + K^{\mathrm{T}}(\gamma - KX)\right) \tag{6}$$

where Φ_λ is the Chambolle's denoising operator, K^{T} is the transpose of the generalized matrix K, and η and ξ are two constants. Here, η and ξ are set to be 1.9608 and 3.9212, respectively, in order to ensure the global convergence of the TwIST algorithm. In the image reconstruction, the formed matrix Cu is employed as the initial value X^0, and the denoising is performed for each image in each iteration calculation. If the difference between the two object functions f^i and f^{i+1} is less than the threshold value or the iteration number reaches the predesigned value N, the object function f is considered to be convergent, and the images are correctly reconstructed.

3. Results and Discussion

To demonstrate the feasibility of our method, we transmit and reconstruct nine face images, and the experimental results are shown in **Figure 3**. It is evident that the reconstructed images retain the high fidelity, and can reflect the original image information. Here, we employ the peak signal-to-noise ratio (PSNR) to illustrate the reconstructed image quality, as given by[22]

$$\mathrm{PSNR} = 10\log 10\frac{1}{\frac{1}{n}\|\tilde{o} - o\|^2} \tag{7}$$

where n is the pixel number of the image, o is the original image signal, and $\tilde{o}$ is the reconstructed image signal by using the measurement image γ. In our experiment, the PSNR value is calculated as 27.38 dB. For many image-processing applications, such a PSNR value is an acceptable quality image reconstruction. Obviously, our technique can directly reconstruct the 3D image information by the encryption and decryption based on the CS algorithm, which differs from previous methods, where only the 2D image information can be reconstructed.[20–24] Here, we use one quantum key to encrypt and decrypt the 3D information that contains nine images, and therefore fewer random codes are required in our scheme, which is very helpful for improving the information transmission bandwidth.

In our experiment, we superimpose the nine images in the space and project them on a plane, that is, our method can compress the 3D data into 2D data, and the data compression ratio can be written as

$$R_{\mathrm{d}} = \frac{N_x \times N_y \times N_z}{N_x \times \left(N_y + N_z\right)} = \frac{N_y \times N_z}{\left(N_y + N_z\right)} \tag{8}$$

Here, the column pixel number of the image N_y is 300 and the image number N_z is 9. Thus, the data compression ratio in our experiment is calculated to be 8.7, which indicates that the information transmission bandwidth in the classical channel can be increased by a factor of 8.7 under the same experimental environment. As shown by Equation (5), the data compression ratio

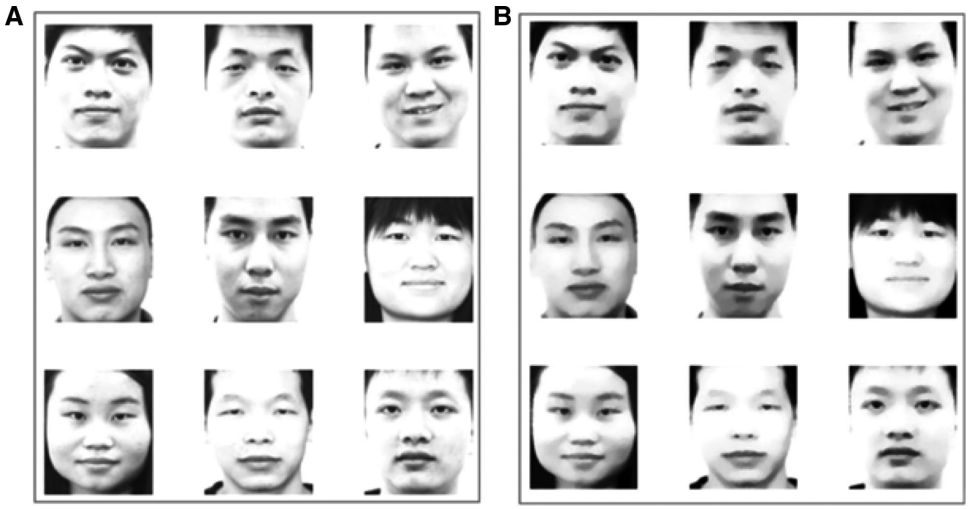

Figure 3. A) Original and B) reconstructed face images by the encryption and decryption based on the compressed sensing (CS) algorithm. Here, the peak signal-to-noise ratio (PSNR) can be up to 27.38 dB.

is related to the image number N_z, and the more compressed images can achieve the higher data compression ratios, and finally obtain the higher information transmission bandwidth.

The QKD system can ensure the unconditional security of the quantum key in the quantum channel,[12,32,33] but the ciphertext in the classical channel may be subjected to the brute force attacks, and therefore the ciphertext security also needs to be considered. The key generated by the QKD system is the true random codes, and thus the attacker usually employs the guess key to reconstruct the image information. To reconstruct the 3D image information clearly, the attacker needs to obtain the correct quantum key but also the correct image number, superimposition method, and image reconstruction algorithm. In mathematics, the normalized correlation coefficient (CC) can illustrate the image similarity, and is expressed as[38]

$$\mathrm{CC} = \frac{\sum_{n=1}^{N}(a_n - \bar{a}_n)(e_n - \bar{e}_n)}{\sqrt{\sum_{n=1}^{N}(a_n - \bar{a}_n)^2}\sqrt{\sum_{n=1}^{N}(e_n - \bar{e}_n)^2}} \tag{9}$$

where a_n and $\bar{a}_n$ (or e_n and $\bar{e}_n$) are one pixel value and mean of original images (or reconstructed images), respectively. We calculate the CC value by only considering the correct rate of random codes in the quantum key, and the calculated result is shown in **Figure 4**A. In statistics, when the CC value is less than 0.3, the reconstructed image is usually considered to be uncorrelated with the original image.[39] In our experiment, the CC value of 0.3 corresponds to the correct rate of approximately 54%. To clearly illustrate the reconstructed image similarity, we present the reconstructed images in some special correct rates of 19.5, 54, 75, 97, and 99.9%, as shown in Figure 4C–F. An attacker cannot obtain any useful information from the reconstructed images when the correct rate is less than 54%. However, when the correct rate is greater than 97%, the face information can be clearly identified from the reconstructed image. In this experiment, we consider that the image information can be well reconstructed with a correlation coefficient value that exceeds 0.8, which corresponds to the correct rate of approximately 93%. Therefore, our technique is robust, which allows a small number of error codes.

As shown in Figure 4, the attacker needs to guess more than 54% correct codes to obtain the useful information from the reconstructed images. In our experiment, one image information consists of 260 × 300 pixels, and it requires 78 000 random binary codes as the key to reconstruct the 3D image information, thus the attacker needs to perform 2^{42120} times. Now, the fastest speed of super computer in the world is usually on the order of 10^{16} (or 10^{17}) times per second.[40] Considering this speed to reconstruct the 3D image information for convenience, the attacker needs to spend at least 2^{42058} (or 2^{42061}) years to finish the image reconstruction, which indicates that completing this arduous task is impossible in the current conditions, let alone the actual calculation speed for the 3D image reconstruction is far much smaller. In previous study, it has shown that attacking the encrypted ciphertext based on the CS algorithm is a non-deterministic polynomial hard (NP-hard) problem.[27] Therefore, our encryption method is hard to be solved by the polynomial due to the inclusion of image number, image superimposition method, and image reconstruction algorithm (i.e., TwIST). A quantum computer cannot effectively attack the NP-complete problem,[41] not to mention the NP-hard problem. Therefore, our encryption and decryption based on CS algorithm can provide the computational security. Actually, the computational security of CS-based encryption has also been demonstrated in the previous studies.[22,27,28] To demonstrate the computational security of our technique, we further calculate the CC value in the cases of 100% random codes and 19.5% correct codes but 80.5% random codes, and the calculated results are shown in **Figure 5**. In our QKD system, the attacker cannot obtain any codes in the quantum channel, but can obtain approximately 19.5% correct codes once the post-processing procedure is removed, and therefore we consider the two special cases in Figure 5. In our simulation of 200 attacks, the CC value is close to 0 for 100% random codes, and is approximately 0.08 for 19.5% correct codes and 80.5% random codes. Therefore, even if a small number of codes are

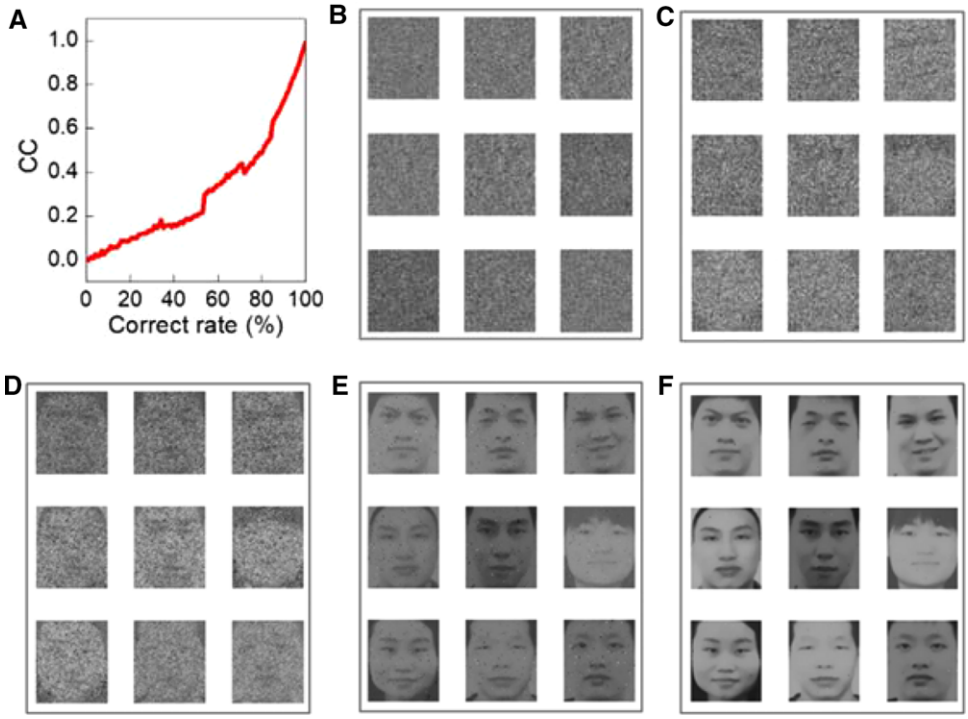

Figure 4. A) Normalized correlation coefficient (CC) as function of the correct rate of the encryption codes, together with B–F) the reconstructed face images with the corresponding correct rate of 19.5% (B), 54% (C), 75% (D), 97% (E), and 99.9% (F).

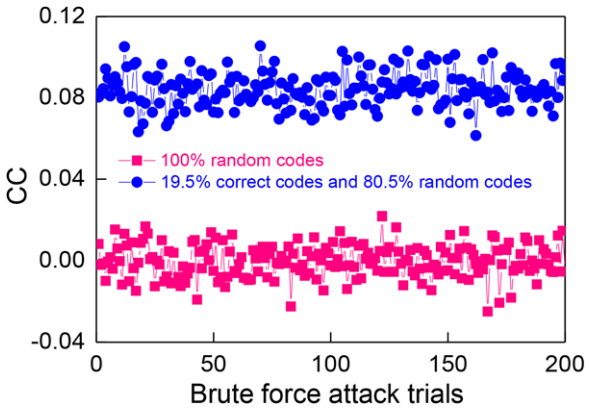

Figure 5. Normalized correlation coefficient (CC) by the brute force attack trials with 100% random codes (pink squares) and 19.5% correct codes and 80.5% random codes (blue circles).

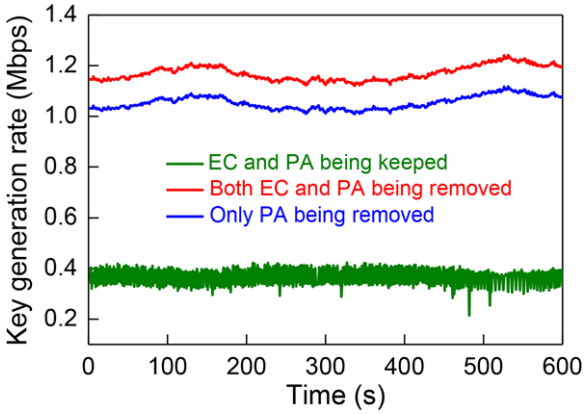

Figure 6. Time-evolution key generation rate (olive line) in the QKD system, together with the privacy amplification (PA) (blue line) and both the error correction (EC) and privacy amplification (red line) being removed in the post-processing procedure.

leaked, the information and communication security can still be protected.

The relatively low key generation rate of current QKD system is a fatal problem for the future practical applications of secure communication. So far, the key generation rate of QKD system can reach 1 Mbps with the distance of 50 km,[42] but such a rate is still not enough for the big data transmission. An important reason is that the error correction and privacy amplification in the post-processing procedure will significantly reduce the key generation rate. Based on the previous discussion and analysis, both the QKD system and CS algorithm can protect the information and communication security, and our image reconstruction method has the robustness, which enables a small number of error codes in the quantum key. Therefore, the error correlation or privacy amplification can be selectively removed to increase the key generation rate. **Figure 6** shows the time-evolution key generation rate in our QKD system, together with only privacy amplification being removed and both error correlation and amplification being removed. When the privacy amplification (or both error correlation and privacy amplification) is removed, the average quantum key rate can be up to 1.05 Mbps (or 1.19 Mbps) from 0.37 Mbps, which is increased by a factor of approximately 2.8 (or 3.2). The combined technique of QKD and CS provides an effec-

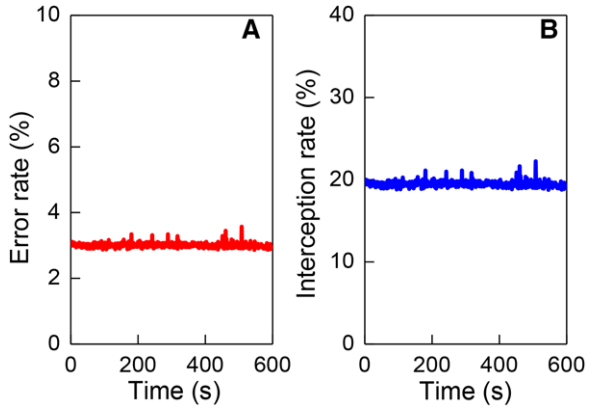

Figure 7. A) Time-evolution error rate and B) interception rate of random codes with both the error correlation and privacy amplification being removed in the post-processing procedure.

tive approach to increase the key generation rate of QKD system, which is very beneficial for improving the information transition bandwidth and the real-time capability of a secure communication system.

Once the error correlation and privacy amplification are removed, two conditions must be satisfied to ensure the security transmission of image information. The first condition is that the receiver can adequately reconstruct the image information in the presence of a certain error rate of random codes, and the second condition is that the attacker can't obtain any useful image information from their reconstructed images. In our QKD system, the sender and receiver have the ability to monitor the error rate and interception rate of random codes when the quantum channel is attacked, which is very helpful in determining whether the random codes in this communication are to be used. Here, the interception rate $h(e)$ corresponds to the correct rate of random codes that we discussed above, and is given by[43]

$$h(e) = -e\log 2(e) - (1-e)\log 2(1-e) \tag{10}$$

where e is the error rate of random codes. **Figure 7** shows the time-evolution error rate and interception rate of random codes with both the error correlation and privacy amplification being removed. The error rate of random codes is stabilized at around 3%, and the interception rate is approximately 19.5%. Obviously, the error rate of 3% can satisfy the condition of 3D image reconstruction (refer to Figure 4E), and the information and communication security still can be guaranteed for the interception rate of 19.5% (refer to Figures 4B,5B). The image information is considered to be well-reconstructed when the correlation coefficient value exceeds 0.8, which corresponds to the error rate of about 7% (refer to Figure 4A), and thus the interception rate is calculated to be 33.6%, which is less than the image similarity limit of a 54% correct rate. Based on these two conditions, the error rate or interception rate of QKD system can be monitored once the quantum channel is attacked. If the error rate (or interception rate) is less than 7% (or 33.6%), these random codes can be employed, otherwise, it is abandoned. Therefore, an important advantage of our scheme is that the image information and communication security can be evaluated in real time by monitoring the QKD system. This real-time information and communication security evaluation by the combination of a QKD system and CS algorithm can introduce a new approach to the QKD system, which will be significant in future practical applications.

In this work, these original nine images are encoded by the same key, and are superimposed in the space by shifting a pixel along the vertical direction. An advantage of this encryption method is that fewer random codes are required, which are equivalent to the pixel number of one image, but the data compression ratio is relatively small. One alternative encryption method is that each original image is encoded by the different keys, and is superimposed in the same space position. This encryption method can obtain the higher data compression ratio, which is equal to the image number, but it needs to employ the more random codes, where the code number is consistent with the pixel number of all the original images. Similar to the former encryption method, this method can also adequately reconstruct the 3D image information and ensure the information and communication security. Therefore, the two different encryption and decryption methods can be selected according to the actual requirement.

In the above study, we consider the static 3D image information and communication security. In the future, our technique can also be applied to the information and communication security of the x-y-t dynamical event, here x and y are the spatial coordinates, and t is the time coordinate. In the measurement of dynamical event, the image sampling, encryption, and compression are simultaneously performed. In the case of the dynamical event that occurs in the range of microseconds, the charge coupled device (CCD) or complementary metal-oxide semiconductor (CMOS) technology can be employed to capture each transient scene, and synchronously send them to a computer to encrypt and compress. Now, the maximum imaging speed of CCD or CMOS technology can be up to 10^7 frames per second.[44] However, if the dynamical event occurs in the range of nanoseconds or picoseconds, the compressed ultrafast photography (CUP) technique can provide a suitable method to simultaneously measure, encrypt, and compress the transient scene,[37,45] where the image encryption and data compression are performed in the optical measurement, which differs from the previously mentioned method by the computer. So far, the CUP technique can capture a time-evolving transient event at a rate of 10^{11} frames per second.

4. Conclusions

To conclude, we have developed a new classical-quantum cryptographic technique to safely transmit the compressed 3D image information by combining the QKD system and CS algorithm. Our technique can not only encrypt and decrypt the compressed 3D image information based on our modified TwIST algorithm, but also can improve the information transmission bandwidth due to the requirement of fewer random codes. Furthermore, our technique can also provide the protection of the information and communication security via CS-based encryption and decryption, and the information and communication security can be evaluated in real time by monitoring the QKD system. Since the information transmission security can be guaranteed and the information transmission bandwidth can be improved, this study can

advance the hybrid classical-quantum cryptographic technique to a new level, and promote the practical applications of information and communication security.

Acknowledgements

C.Y. and Y.D. contributed equally to this study. C.Y. wrote the program, performed the experiments, analyzed the data, and prepared the manuscript. Y.D. built the experimental system, analyzed the data, and prepared the manuscript. J.L. wrote a part of program. F.C. performed some of experiments. D.Q. performed some of experiments. T.J. analyzed the data. S.Z. contributed to the data analysis and manuscript revision. Z.S. contributed to the experimental design, image reconstruction, data analysis, and manuscript revision. W.C. contributed to the experimental design, data analysis, and manuscript revision. Z.Y. performed some of theoretical calculations. S.W. performed some of experiments. Z.H. contributed to the experimental design. G.G. contributed to the experimental design. L.V.W. contributed to the conceptual system and manuscript revision. This work was supported partly by National Natural Science Foundation of China (Nos. 11474096, 11774094, 61627820, 61675189, 61622506, 61475148, 61575183), Science and Technology Commission of Shanghai Municipality (Nos. 16520721200, 17ZR1446900), National Key Research and Development Program of China (Nos. 2016YFA0302600, 2016YFA0301702), and "Strategic Priority Research Program (B)" of the Chinese Academy of Sciences (No. XDB01030100). All the research participants confirm that they are aware and agree that their images in Figures 2–4 are used for the research description and that their pictures are shown in this article.

Conflict of Interest

The authors declare no conflict of interest.

Keywords

compressed sensing, image encryption and decryption, information and communication security, quantum key distribution

Received: April 19, 2018
Revised: May 6, 2018
Published online:

[1] P. W. Shor, *SIAM J. Comput.* **1997**, *26*, 1484.
[2] S. Imre, L. Gyongyosi, *Advanced Quantum Communications—An Engineering Approach*, Wiley-IEEE Press, Hoboken, NJ **2012**.
[3] W. Liu, J. Peng, C. Wang, Z. Cao, D. Huang, D. Lin, G. Zeng, *Sci. China Phys. Mech. Astron.* **2015**, *58*, 020301.
[4] G. L. Long, X. S. Liu, *Phys. Rev. A* **2002**, *65*, 032302.
[5] L. Gyöngyösi, S. Imre, *Proc. SPIE* **2014**, *10*, 10.
[6] A. Mraz, S. Imre, L. Gyöngyösi, 24th European Signal Processing Conference (EUSIPCO), Budapest, Hungary **2016**, pp. 498–502.
[7] Y. B. Sheng, L. Zhou, *Sci. Bull.* **2017**, *62*, 1025.
[8] D. Ristè, M. P. Da Silva, C. A. Ryan, A. W. Cross, A. D. Córcoles, J. A. Smolin, B. R. Johnson, *npj Quantum Inform.* **2017**, *3*, 16.
[9] J. F. Fitzsimons, *npj Quantum Inform.* **2017**, *3*, 23.
[10] Y. B. Sheng, L. Zhou, *Sci. Rep.* **2015**, *5*, 7815.
[11] F. G. Deng, G. L. Long, X. S. Liu, *Phys. Rev. A* **2003**, *68*, 042317.
[12] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, *Rev. Mod. Phys.* **2002**, *74*, 145.
[13] C. E. Shannon, *Bell Labs Tech. J.* **1949**, *28*, 656.
[14] T. Honjo, S. W. Nam, H. Takesue, Q. Zhang, H. Kamada, Y. Nishida, O. Tadanaga, M. Asobe, B. Baek, R. Hadfield, S. Miki, M. Fujiwara, M. Sasaki, Z. Wang, K. Inoue, Y. Yamamoto, *Opt. Express* **2008**, *16*, 19118.
[15] L. Gyongyosi, *Improved Long-Distance Two-Way Continuous Variable Quantum Key Distribution over Optical Fiber*, Frontiers in Optics/Laser Science XXIX (FiO/LS), Orlando, USA **2013**.
[16] V. L. Kurochkin, A. V. Zverev, Y. V. KurochkinI, I. I. Ryabtsev, I. G. Neizvestnyi, R. V. Ozhegov, G. N. Gol'tsman, P. A. Larionov, *Optoelectronics Instrum. Data Process.* **2015**, *51*, 548.
[17] D. J. Bernstein, *Introduction to Post-QuantumCryptography*, Springer-Verlag, Berlin, Heidelberg **2009**.
[18] T. S. Thangavel, A. Krishnan, *Int. Conf. Comput. Commun. Networking Tech.*, Karur, India **2010**.
[19] S. Ranganathan, N. Ramasamy, S. K. K. Arumugam, B. Dhanasekaran, P. Ramalingam, V. Radhakrishnan, R. Karpuppiah, *Int. J. Computer Sci. Issues* **2010**, *7*, 148.
[20] N. Zhou, A. Zhang, J. Wu, D. Pei, J. Yang, *Optik – Int. J. Light Electron Opt.* **2014**, *125*, 5075.
[21] X. Zhang, Y. Ren, G. Feng, Z. Qian, *7th Int. Conf. Intel. Inf. Hiding and Multimedia Sig. Process.*, Dalian, China **2011**.
[22] A. Orsdemir, H. O. Altun, G. Sharma, M. F. Bocko, *Military Commun. Conf.*, San Diego, USA **2008**.
[23] A. M. Abdulghani, E. Rodriguez-Villegas, *Conf. Proc. IEEE Eng. Med. Bio. Soc.*, Buenos Aires, Argentina **2010**.
[24] R. Huang, K. Sakurai, *7th Int. Conf. Intel. Inf. Hiding and Multimedia Sig. Process.*, Dalian, China **2011**.
[25] E. J. Candès, J. Romberg, T. Tao, *IEEE Trans. Inf. Theory* **2006**, *52*, 489.
[26] D. L. Donoho, *IEEE Trans. Inf. Theory* **2006**, *52*, 1289.
[27] Y. Rachlin, D. Baron, *2008 46th Annual Allerton Conference on Communication, Control, and Computing*, IEEE **2009**.
[28] M. R. Mayiami, B. Seyfe, H. G. Bafghi, *2013 Iran Workshop on Communication and Information Theory (IWCIT)*, Tehran, Iran **2013**.
[29] C. Wang, B. Zhang, K. Ren, J. M. Roveda, *IEEE Trans. Emerg. Top. Comput.* **2013**, *1*, 166.
[30] M. Zhang, M. M. Kermani, A. Raghunathan, N. K. Jha, *Int. Conf. VLSI Design and Int. Conf. Embedded Syst.*, Pune, India **2013**.
[31] V. Cambareri, M. Mangia, F. Pareschi, R. Rovatti, *IEEE Trans. Signal Process.* **2015**, *63*, 2183.
[32] N. Zhou, A. Zhang, F. Zheng, L. Gong, *Opt. Laser Tech.* **2014**, *62*, 152.
[33] D. Xiao, L. Wang, T. Xiang, Y. Wang, *Opt. Laser Tech.* **2017**, *91*, 212.
[34] X. Song, H. Li, C. Zhang, D. Wang, S. Wang, Z. Yin, W. Chen, Z. Han, *Chin. Opt. Lett.* **2015**, *13*, 012701.
[35] X. Lu, L. Zhang, Y. Wang, W. Chen, D. Huang, D. Li, S. Wang, D. He, Z. Yin, Y. Zhou, C. Hui, Z. Han, *Sci. China Phys. Mech. Astron.* **2015**, *58*, 120301.
[36] J. M. Bioucas-Dias, M. A., T. Figueiredo, *IEEE Trans. Image Process.* **2007**, *16*, 2992.
[37] L. Gao, J. Liang, C. Li, L. V. Wang, *Nature* **2014**, *516*, 74.
[38] Y. Yue, J. Yu, Y. Wei, X. Liu, T. Cui, *JCIS* **2013**, *9*, 7325.
[39] R. Taylor, *JDMS* **1990**, *6*, 35.
[40] China's Sunway-TaihuLight named world's fastest supercomputer, http://english.gov.cn/news/photos/2016/06/20/content_281475376099575.htm (accessed: December 2016).
[41] C. H. Bennett, E. Bernstein, G. Brassard, U. Vazirani, *SIAM J. Comput.* **1997**, *26*, 1510.
[42] L. C. Comandar, B. Fröhlich, M. Lucamarini, K. A. Patel, A. W. Sharpe, J. F. Dynes, Z. L. Yuan, R. V. Penty, A. J. Shields, *Appl. Phys. Lett.* **2014**, *104*, 021101.
[43] M. Tomamichel, R. Renner, *Phys. Rev. Lett.* **2011**, *106*, 110506.
[44] Y. Kondo, K. Takubo, H. Tominaga, *Shimadzu Rev.* **2012**, *69*, 285.
[45] J. Liang, C. Ma, L. Zhu, Y. Chen, L. Gao, L. V. Wang, *Sci. Adv.* **2017**, *3*, e1601814.

