Transmission of hidden images within noise

Steven Johnson, Alex McMillan*, Stefan Frick*, John Rarity*, Miles Padgett
Physics and Astronomy, University of Glasgow, Glasgow, Scotland. UK
*School of Electrical, Electronic and Mechanical Engineering, University of Bristol, Bristol. UK

ABSTRACT

The secure transmission of an image can be accomplished by encoding the image information, securely communicating this information, and subsequently reconstructing the image. As an alternative, here we show how the image itself can be directly transmitted while ensuring that the presence of any eavesdropper is revealed in a way akin to quantum key distribution. We achieve this transmission using a photon-pair source with the deliberate addition of a thermal light source as background noise. One photon of the pair illuminates the object, which is masked from an eavesdropper by adding indistinguishable thermal photons, the other photon of the pair acts as a time reference from which the intended recipient can preferentially detect the image carrying photons. These reference photons are themselves made sensitive to the presence of an eavesdropper by traditional polarisation-based QKD encoding. Interestingly the security encoding is performed in the two-dimensional polarisation-basis, but the image information is encoded in a much higher-dimensional, hence information-rich, pixel basis. In our example implementation, our images have more than 100 independent pixels. Beyond the secure transmission of images, our approach to the distribution of secure high-dimensional information may create new high-bandwidth approaches to traditional QKD.

Keywords: Quantum Key Distributions, Noise free imaging

1. INTRODUCTION

The transmission of information via a quantum-secure protocols is becoming a major technology in secure communications[1]. Techniques based on quantum key distribution (QKD) are set to become mainstream for the defence and finance industries to securely send information by know if the encryption key has been intercepted, albeit one limitation is the data transmission speed. In parallel to advances in this communication technology, advances in quantum imaging are using single photons to produce enhancements in imaging performance and use correlation between photons to enable images to be produced in challenging, high-noise, regimes[2]. Bringing these two technologies together to encode photons in a high dimensional basis, such as an image, may both greatly increase the data capacity of a communication system and allow secure, and direct image transmission.

QKD system based upon BB84 use the polarisation state of the light to encode a photon in a binary state corresponding to one bit per photon. As with all QKD systems the key aspect is that this polarisation information can be encoded in at least two mutually unbiased bases, in this case two bases from, vertical: horizontal, or diagonal: anti-diagonal, or right-circular: left-circular polarisations. The sender and intended recipient transmit and measure in a random series of these bases and subsequently compare their results. An eavesdropper can also make measurements but when they re-transmit, they must select a basis and in doing so corrupt the channel, hence revealing their presence. The requirement for single-photon operation, inherent transmission/detection losses, and various necessary error corrections means that the secure bit rate is much smaller than a classical, albeit insecure, system.

To increase the data rate of QKD there has been much work on using higher dimensional, but again mutual unbiased basis[3], e.g. time: frequency[4], orbital angular momentum: angle[5], position: transverse momentum[6]. In all these examples the information is transmitted with high fidelity with the security being introduced by the random selection of transmission and detection basis.

In this present work we take a different approach which builds upon our previous work for hiding low flux images in noise. This earlier work used a photon pair source producing time-correlated signal and idler beams. The signal beam was used to create an image by transmission through a patterned mask and the idler beam was used to trigger a detector to record the position of the signal photons and hence the image. This image was hidden from eavesdroppers by deliberately adding background light, hence only recipient with access to the idler trigger photons could isolate the true image from the background noise[7]. This embedding the image in noise approach gives some element of security, but in principle an eavesdropper could intercept the trigger photons, use them to extract their own image and then re-transmit both the image and the trigger to the intended recipient. We now overcome this security limitation by polarisation encoding the heralding photons and hence, inspired by BB84, ensuring that the presence of any eavesdropper is revealed[8].

Quantum Sensing, Imaging, and Precision Metrology II, edited by Jacob Scheuer,
Selim M. Shahriar, Proc. of SPIE Vol. 12912, 129120U · © 2024
SPIE · 0277-786X · doi: 10.1117/12.3000546

Interestingly, in our approach, although the information is recorded in a high-dimension Hilbert space (i.e. position) the security is ensured by a traditional QKD-inspired approach within a 2-dimensional space (i.e. polarisation). In essence the trigger photons are secured by their polarisation to give temporal information, from which to extract the spatial information from the time-correlated photon. Inherent to our security is the need for background noise being added to the information, i.e. the noise is a virtue not a limitation. This need for noise makes our approach particularly suited to situations where the background noise is inherent to the operation, such as optical transmission in free-space.

2. METHODOLOGY

The core components of the system were: the spontaneous parametric down conversion (SPDC) system, the polarisation encoded heralding arm, and image transmission and imaging arm. The temporally correlated photon-pairs are split between the QKD heralding arm and the image transmission arm. An experimental schematic is shown in figure 1.

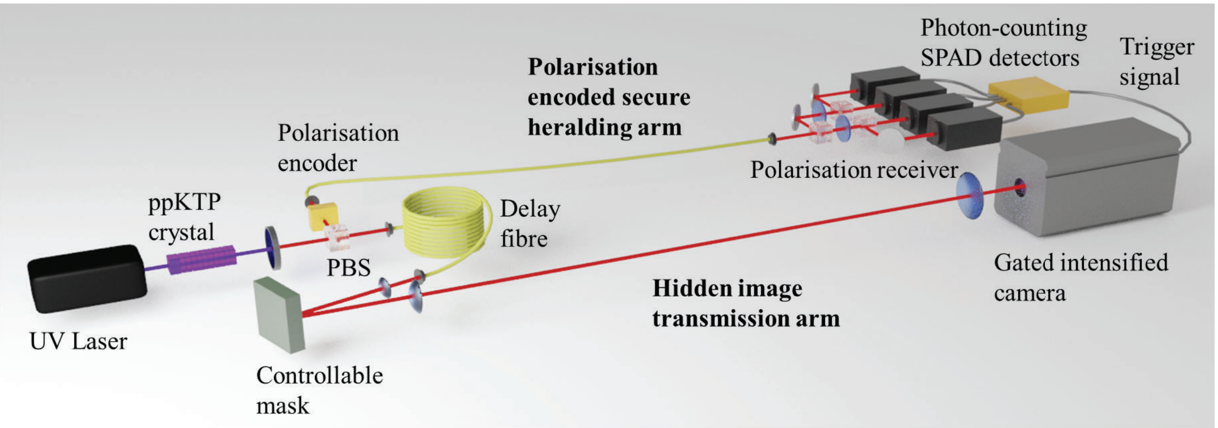

Figure 1. An illustration of the experimental set up. The UV laser passing through the ppKTP crystal produced a photon-pair. One photon travelled through a rotating half-wave plate as a polarisation encoder and transmitted through an optical fibre to a polarisation detection scheme with a SPAD detector for each polarisation state, the signals from the detectors are summed and output to trigger the camera. The other photon travels through the imaging arm, where the image is formed by a digital micromirror device and projected image onto a gated intensified camera.

The SPDC source comprises a 405 nm diode laser pumping a ppKTP type-II non-linear crystal. The crystal has 9.8 µm polling and is 30 mm long. The residual UV pump beam is filtered out with a long-pass wavelength filter. The signal and idler beams, centred at 810nm but with bandwidth more than 100nm, have orthogonal polarisation, thereby the photon-pairs can be separated using a polarising beam splitter (PBS) and coupled into separate optical fibres REF. The polarisation encoded heralding arm uses a rotating half-waveplate to set the polarisation of the light to be horizontal (H), vertical (V), diagonal (D) or anti-diagonal (A). The light is focused into a single mode optical fibre, where a manual fibre polarisation controller is used to ensure the polarisation was faithfully transmitted. The receiver uses a 50:50 beam-splitter to make a random choice for the direction of a photon. On one output is a PBS to measure the H and V polarisation states, the other side has a half-waveplate to rotate the polarisation by 45° and a further PBS to measure the D and A polarisation states. The photon measurements are made using single-photon avalanche diode (SPAD) photon-counting module (Excelitas SPCM-AQRH). The signals from the four SPAD detectors are summed using a 4-channel OR-gate, where the output of the OR-gate was used to trigger the camera in the imaging arm.

The image transmission arm first passed the photons through a long single mode fibre (50 m) that acts as a delay-line to ensure the light arrives slightly after the heralding signals. The light from optical fibre is collimated and illuminates a digital micro-mirror device, acting as a programmable mask to generate the image to be transmitted to the camera. The image is then transmitted, in our case, over 1.8 m through free space and imaged onto a gated intensified CCD camera (Andor iStar 334T). The camera has a gated intensifier that can be activated such that a single incident photon produces an optical signal at the CCD, substantial above the noise floor of the device. The gating enables to camera to remain on for 10 ns after the heralding signal has arrived, such that the paired photon would arrive during this period. The camera was read out every 1 second and the frame stored. The maximum gating rate of the camera is ≈ 200 kHz. The image signal is hidden from an eavesdropper by adding additional background light, which in our case is achieved using an LED at the signal wavelength (800 nm).

The LED is controlled with an I/O device (NI USB-6361), calibrated to give a known level of background light. A QKD approach is used to securely send photons via optical fibre to the receiver. This could be used to determine if an eavesdropper is intercepting the heralding photons. The gated intensified camera takes an image when triggered by the polarisation encoded heralding arm. The digital delay within the camera is set such that the temporally correlated photon is captured during the activation of the gated intensified camera. Background illumination is added via optical illumination to hide the intended image such that the signal is well below the shot-noise measured and only recoverable using the heralding signal, see figure 2. By recording the send order of the polarisation states and comparing the states after optical transmission it is possible to identify if an eavesdropped has been accessing the heralding channel.

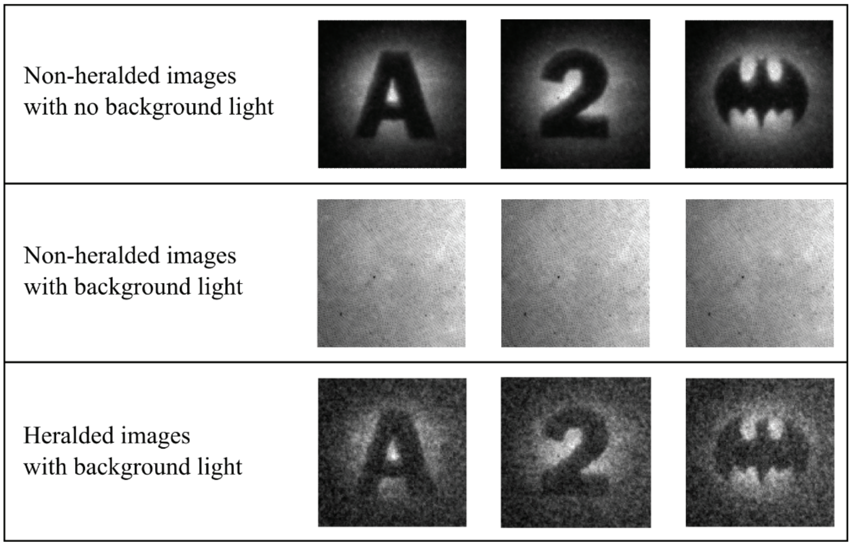

Figure 2. Non-heralded and heralded images obtained from the summation of single photon events with and without background light.

3. RESULTS

The system was run measuring one polarisation state at a time, the triggers due to this polarisation state were used to trigger the camera. When the polarisation state transmitted in the heralding arm state was the same as that used to trigger the camera there were around 80 000 counts per second measured, hence the camera would be triggered to collect those photons. For example, when the H polarisation state is sent it would be expected to see approximately 50% of the signal on the H channel, with 25% on both the D channel and A channel, with a near-zero signal on the V channel. This is shown in figure 3a, where the photons are measured directly with the camera, the transmission of the polarisation state in the heralding arm are indicated by the letter used the image projection of that state, and the measured image for each polarisation channel is shown. In these time-gated images a 10 ns gate time is used such that the noise can be rejected. Without the gating, the addition of the background noise to the imaging channel obscures the image such that the eavesdropper would be unable to detect the image without the heralding signal, see figure 3b.

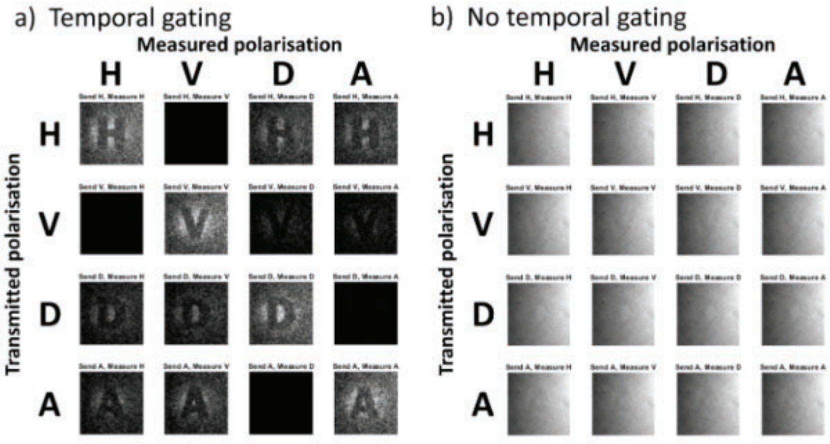

Figure 3. Images obtained from the summation of single photon events with the transmission and detection of the heralding arm as show. Figure a) shows the heralded gated image, figure b) show the images with the same level of added noise but no heralding signal and hence no gating of the camera.

4. CONCLUSIONS

We have demonstrated that images produced from a correlated photon-pair source can be hidden within a background of optical noise, where the heralding channel is protected by sending polarisation encoding states in a similar manner to QKD. The system used spontaneous parametric down-conversion to create photon-pairs where the photons were split between a polarisation encoded heralding arm and an image projection arm. The polarisation state encoding allows a post-measurement comparison of states between the sender and receiver to ensure the photons were sent securely. The imaging arm maintain covertness by hiding the image photons such that they cannot be differentiated from the background via any temporal or spectral filtering. This transmission of images can be used for the covert communication of information in a secure way, where the information content is limited by the ability to discern photons on the camera.

Whilst this work demonstrates that the system will work in principle there is no demonstration of speed or robustness presented. The addition of an eavesdropper has not been shown here but in the spirit of BB84, would be clear from a deviation of signals from the expected polarisation states during the measurement of the heralding arm. These limitations are not fundamental problems that undermine the concept, and the results are a clear indication of a secure image transmission system.

REFERENCES

[1] Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N. and Peev, M., “The security of practical quantum key distribution,” Rev. Mod. Phys. **81**(3), 1301–1350 (2009).
[2] Gregory, T., Moreau, P. A., Toninelli, E. and Padgett, M. J., “Imaging through noise with quantum illumination,” Science Advances **6**(6), eaay2652 (2020).
[3] Cerf, N. J., Bourennane, M., Karlsson, A. and Gisin, N., “Security of Quantum Key Distribution Using d-Level Systems,” Phys. Rev. Lett. **88**(12), 127902 (2002).
[4] Ali-Khan, I., Broadbent, C. J. and Howell, J., “Large-Alphabet Quantum Key Distribution Using Energy-Time Entangled Bipartite States,” Phys. Rev. Lett. **98**(6), 060503 (2007).
[5] Mirhosseini, M., Magaña-Loaiza, O. S., O’Sullivan, M. N., Rodenburg, B., Malik, M., Lavery, M. P. J., Padgett, M. J., Gauthier, D. J. and Boyd, R. W., “High-dimensional quantum cryptography with twisted light,” New J. Phys. **17**(3), 033033–12 (2015).
[6] Tentrup, T. B. H., Luiten, W. M., Meer, R. van der, Hooijschuur, P. and Pinkse, P. W. H., “Large-alphabet quantum key distribution using spatially encoded light,” New J. Phys. **21**(12), 123044 (2019).
[7] Johnson, S., McMillan, A., Frick, S., Rarity, J. and Padgett, M., “Hiding images in noise,” Opt. Express **31**(4), 5290 (2023).
[8] Bennett, C. H. and Brassard, G., “Quantum cryptography: Public key distribution and coin tossing,” Theor. Comput. Sci. **560**, 7–11 (2014).