Considerations for the extension of coherent optical processors into the quantum computing regime

Article (Accepted Version)

Considerations for the extension of coherent optical processors into the quantum computing regime

Rupert C. D. Young, Philip M. Birch, Chris R. Chatwin

Department of Engineering and Design,
School of Engineering and Informatics
University of Sussex,
Brighton, United Kingdom, BN1 9QT
E-mail: r.c.d.young@sussex.ac.uk

ABSTRACT

Previously we have examined the similarities of the quantum Fourier transform to the classical coherent optical implementation of the Fourier transform (R. Young et al, Proc SPIE Vol 87480, 874806-1, -11). In this paper, we further consider how superposition states can be generated on coherent optical wave fronts, potentially allowing coherent optical processing hardware architectures to be extended into the quantum computing regime. In particular, we propose placing the pixels of a Spatial Light Modulator (SLM) individually in a binary superposition state and illuminating them with a coherent wave front from a conventional (but low intensity) laser source in order to make a so-called 'interaction free' measurement. In this way, the quantum object, i.e. the individual pixels of the SLM in their superposition states, and the illuminating wavefront would become entangled. We show that if this were possible, it would allow the extension of coherent processing architectures into the quantum computing regime and we give an example of such a processor configured to recover one of a known set of images encrypted using the well-known coherent optical processing technique of employing a random Fourier plane phase encryption mask which classically requires knowledge of the corresponding phase conjugate key to decrypt the image. A quantum optical computer would allow interrogation of all possible phase masks in parallel and so immediate decryption.

Keywords: coherent optical processing, optical quantum computing, superposition states, multiple photon states, interaction free measurements, coherent optical Fourier transform, spatial light modulators

1. INTRODUCTION

In a previous paper[1], we have drawn attention to the similarity of the quantum Fourier transform (QFT) to the coherent optical implementation of the Fourier transform. The optical hardware for the implementation of both was shown to be identical, the essential difference being that the QFT operates on data in a superposition state. In this paper we wish to further examine how classical coherent optical processing architectures may be extended to operate on data in a superposition state and so exploit the computational advantages of operating in the quantum regime.

The manipulation of the complex amplitude of a coherent wave front forms the basis of coherent optical processing techniques. Central to these methods has been the ability of a converging lens to form in its back focal plane the complex two-dimensional Fourier transform of an aperture function placed in its front focal plane[2]. In addition, the recording of the Fourier domain complex field via carrier wave holographic methods has led to the development of the two lens 4-focal length coherent optical processor[2] which is shown schematically in Figure 1. It is well known that this arrangement can be employed to implement the two dimensional correlation between a reference object and an input scene[3]. The correlation signal in the output plane then indicates the presence and location of the reference object in the input scene. This search capability can be exploited to implement one of the well-known quantum algorithms, namely the Grover algorithm[4], as will be shown in the next section. Extension of the capability of the coherent optical correlator hardware to the implementation of algorithms requiring entanglement of the data, such as the Shor algorithm[5], would require superposition states to be propagated through the optical system. To generate these states we propose placing the pixels of a Spatial Light Modulator (SLM), located in the frequency plane of the 4-f optical system, individually in a binary superposition state. A conventional (but low intensity) laser source would be employed as the coherent source and used to make a so-called 'interaction free' measurement of the SLM pixels. In this way, the quantum object, i.e. the individual superposition states of the SLM pixels, become entangled onto the illuminating wavefront. We show that, if this were possible, it would allow the extension of coherent processing architectures into the quantum computing regime and we describe a simple 'thought experiment' to illustrate how such a capability could be exploited.

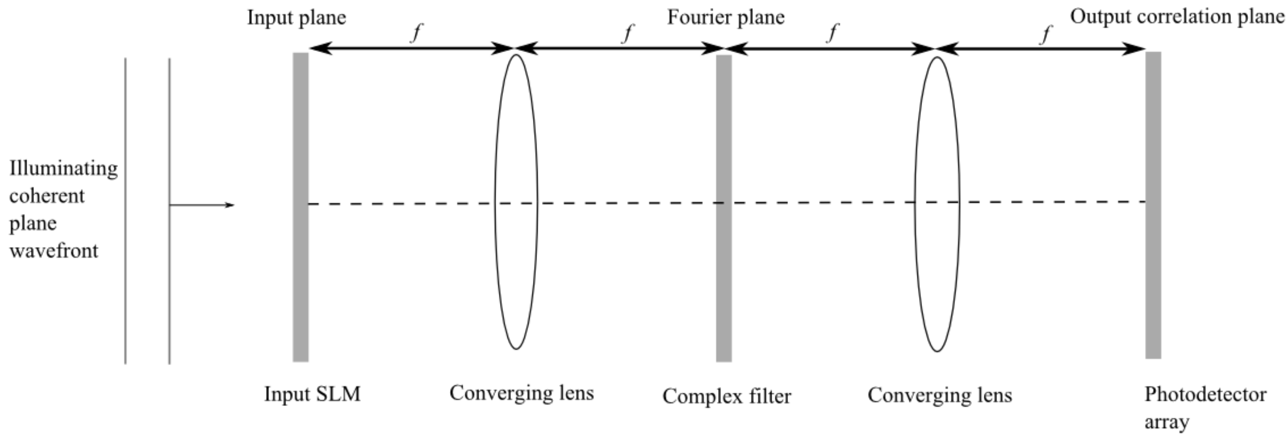

Figure 1. Canonical 4-f coherent optical processor

2. OPTICAL IMPLEMENTATION OF QUANTUM ALGORITHMS

The Grover quantum search algorithm[4], was one of the initial algorithms devised that demonstrated the potential of quantum computing methods to accelerate computing rates dramatically over existing methods. The algorithm allows the location of a data item in an unordered database. A good example is the classical problem of locating the name of an individual in an alphabetically ordered phone book given only their telephone number. Classically, this would require, on average, N/2 searches to locate the individual. In contrast, the Grover quantum algorithm can complete the search in $O(N^{1/2})$. Interestingly, the Grover quantum algorithm employs quantum interference but not entanglement[6]. Each data item is associated with a quantum state and a system of the superposition of all N quantum states is generated. The probability amplitude of the sought for item is amplified by an iterative process. Once this is near unity, the state of the system is measured and the target item identified[4]. The algorithm does require, however, the target item to be initially labelled by inverting the phase of its associated quantum state[7]. In the second step, phase information is converted to amplitude information by inverting all amplitudes about the average amplitude. An iterative process is implemented that amplifies the amplitude of the target object to near unity at which point measurement of the wavefront leads its collapse at a position corresponding to the location of the target object in the database with near certainty. Bhattacharia et al.[7], and Hijmans et al.[6] have shown, however, that a classical coherent optical system can implement the search in a very similar way by employing a classical optical wavefront, in contrast to a wavefunction. Their proposed system is iterative, to mimic more closely the Grover algorithm but, essentially, it is very closely related to a classical Zernike phase contrast arrangement which has been used for many years to detect spatial density changes in microscopy by converting phase changes generated by the spatial density variations of cells in the input field of view to intensity changes which are clearly visible. The implementation is thus based on a 4-f optical system. The input plane contains the data to be searched with the target location marked by a phase notch (the reader may well wonder how the phase notch can be placed over the location of the target data entry location if this is unknown. In the literature, the phase notch is placed by a so-called 'oracle' which is invoked before initiation of the search algorithm). The light field is Fourier transformed by the first lens, and in the spatial frequency plane of this lens a π/2 phase change is imparted to the zero frequency term. As in the Zernike system, this results in any phase profiles in the input plane being imaged in the output plane as intensity changes. Hence the location of the phase notch can be determined and so the location of the data entry (although the method of locating the output intensity spike in the output plane requires to be given a little further thought which we do shortly).

However, from these considerations, it immediately becomes clear that the 4-f optical system can be used directly as a correlator to accomplish the search (and without the necessity to place a phase notch over the location of the target data entry!). Take the phone book search as an example. A matched filter is made of an image of the phone number that is sought in the database by recording the phase conjugate of its Fourier spectrum in the spatial frequency plane of the 4-f optical system (such as by a holographic method, as originally proposed by Vander Lugt[3].) We proceed by loading data from the phone book, one frame at a time, onto an input SLM. Upon illumination with a coherent wavefront, the correlator will generate a correlation peak in the output plane if the target data (i.e. the telephone number) is contained in the input plane and, further, the correlation peak will be shifted to a position in the output plane corresponding to the location of the target data in the input plane, so indicating the position in the database of the name and address of the individual whose telephone number was recorded as the matched filter. Practicalities, such as constraints on the physical size of the optical system, limit the amount of data that can be loaded onto a single input frame. Also, no doubt, the data would be encoded in a more abstract form in a real application. However, the principle is demonstrated that by classical coherent optical methods the search for the unknown location of a data item in a data field can be performed in parallel without the need for a sequential search method. This is because the Grover algorithm does not require entanglement of the data, in contrast to other quantum algorithms, that will be considered shortly.

A final point that must be addressed is the objection that, since the output correlation peak can be located anywhere on a N pixel output array, to find its position would need, on average, N/2 pixels to be searched i.e. require the same number of sequential operations as a serial search. This would be true for a direct pixel search. However, assuming we only have one data item within an input frame, the single correlation peak may be located by projecting it onto the x- and y-axes of the output plane (which will be of length $N^{1/2}$ pixels for a square N pixel array). Its location then involves counting along these axes until it is found which, again on average, will require 2 x $N^{1/2}/2$ operations. This is, rather interestingly, $O(N^{1/2})$, i.e. the same as for the Grover algorithm. Clearly though, the classical implementations of the Grover algorithm are limited by the fact they have to access data stored conventionally in a physical memory rather than data stored in superposition states in a quantum memory which could store exponentially more data with the same physical resource.

Another quantum algorithm of major importance is the Shor algorithm[8]. This is because it addresses the difficult problem of factoring a large integer number into its prime factors which, via conventional means, is a computation that scales exponentially with the size of integer to be factored. The problem is of practical importance because such factorisation would allow public-key encryption methods to be defeated.

Details of the Shor algorithm are given by Shor[8], Ekert and Jozsa[9] and is summarised in our previous paper[1]. The algorithm requires entanglement of bits in a quantum register and unitary operations on these data that perform parallel computations of the superposition state of the data without collapse of the wavefunction. In order to factor a number N, a number q is chosen such that $N^2<q<2N^2$ to create a state in a quantum register[10]:

$$|\psi_1\rangle = \frac{1}{\sqrt{q}}\sum_{a=0}^{q-1}|a,0\rangle \quad (1)$$

from which is computed (by the quantum computer maintaining the superposition state):

$$|\psi_2\rangle = \frac{1}{\sqrt{q}}\sum_{a=0}^{q-1}|a, x^a \bmod N\rangle \quad (2)$$

This operation results in a periodic function that can be related to the order, r, from which a factor of N can be derived[8,9,10]. However, the period cannot be extracted directly from equation (2) since this represents a superposition state of many functions computed from equation (1) in parallel by the quantum computer. The solution devised by Shor was to perform a QFT on the superposition state represented by equation (2) to yield:

$$\left|\psi_3\right\rangle = \frac{1}{\sqrt{q}} \sum_{m=0}^{q-1} \sum_{a=0}^{q-1} e^{-j\pi a m/q} \left|m, x^a \bmod N\right\rangle \tag{3}$$

The state that is periodic in equation (2) will be Fourier transformed to a peak, the location of which in the output plane corresponds to its frequency. All other states that are not periodic will not Fourier transform to a peak and so have less probability of detection when the wavefunction is collapsed by a measurement of the output. The high probability of collapse at the location of the peak of the wavefunction will allow the frequency, and hence the value of r, to be determined in turn allowing a factor of N to be found.

The critical role of the QFT in the Shor algorithm is thus clear. A general problem in quantum computing is that calculations may be performed in a superposition state but to extract information from the calculation requires a measurement to be made and so a collapse of the wavefunction. The Shor algorithm ensures the solution to the problem has a periodicity which can be Fourier transformed to a peak in the wavefunction which has a high probability of detection when a measurement is made. Thus useful information can be extracted from a superposition state.

However, essential to the performance of the Shor algorithm is the entanglement of data bits in a quantum register and the maintenance of the superposition state through unitary operations such as the QFT. Optical implementations of the Shor algorithm have been reported but the technical difficulty in generating entangled photons has strictly limited the bit length of the input data[11]. In the following section we discuss an alternative suggestion for producing the required entanglement of qubits using a so-called "interaction free measurement" of SLM pixels individually held in a binary superposition state. Further, the entanglement so imparted to a wavefunction can be propagated through phase modulating optical components which thus allow unitary operations to be performed on the superposition states in parallel, so exponentially increasing the computational power of the optical processor.

3. QUBIT ENTANGLEMENT IN AN OPTICAL WAVEFRONT PROCESSOR

A new means of producing the required qubit entanglement is proposed in this paper. Consider a binary phase modulating SLM. In conventional operation, the pixels would be in one of two states such that, ideally, a coherent wavefront interacting with each pixel (either transmitted or reflected by the device) would, depending on the pixel state, be unaffected in local phase or shifted by π radians i.e. half a wavelength. Suppose that the pixel could be placed in a superposition state of 0 and π phase modulation, so as to produce a qubit. It is necessary to entangle the SLM qubits to provide the superposition states required for quantum algorithms such as the Shor factorisation method. If the SLM (with N qubit pixels) is illuminated by the wavefunction resulting from a single photon, the wavefunction will reflect from the SLM in a superposition state of the 2^N states possible for the binary SLM qubits and so entangle the N qubits, thus providing what is known as an interaction-free measurement[12,13,14]. Thus a wavefunction would be produced that can be written:

$$\left|\psi\right\rangle = \sum_{n=0}^{N-1} x_n \left|n\right\rangle \tag{4}$$

The wavefunction, maintaining its superposition state derived from its reflection from the SLM qubits, will propagate through the optical processor. This will generate the required phase modulations of the wavefunction to implement the required unitary operations to realise a particular quantum algorithm. For example, a QFT operation may be performed, by a simple converging lens, to yield a superposition state in a Fourier plane:

$$\left|\Psi\right\rangle = \sum_{n=0}^{N-1} e^{-j\frac{2\pi nk}{N}} \left|\psi\right\rangle \tag{5}$$

The wavefunction will collapse at the output detector when an intensity measurement is made but, as we have seen, this can be arranged to provide specific information such as, for instance, the periodicity of one superposition state of the wavefunction.

Until now we have considered the wavefunction from a single photon and its self-interference as it propagates through the optical system. However, we can then see no reason that multiple (fully coherent) photons should not be introduced simultaneously into the optical processor, behave in identical ways and so allow classical detection, rather than single photon counting detection. By "fully coherent" we mean originating from a single frequency laser source within an interval less than the coherence time of the laser, which for a modern laser could be of the order of 1 μsec, i.e. a 300 m coherence length, within which time more than 2 x 10^9 visible wavelength photons could be provided by a source of only 1 mW power. This would then allow a conventional coherent source, optics and detector to be employed in the processor. To help lend some support to the possibility of entangling SLM qubits optically, with a multiple photon source, we quote from a recent article by Kwiat[14]:

"If such systems (here discussing a physical system in a superposition state) are evaluated using interaction-free measurement schemes, then the two sub-systems – quantum object and the interrogating light – become entangled. In fact, although we have not discussed it at all here, for sufficiently large N (number of measurement cycles), the interaction-free measurement methods even work for multi-photon states, even for dim classical pulses. Therefore, combining such an input with a quantum object, one is able to transfer quantum superposition of the latter into the former."

Of course, the technically demanding aspect is to provide an SLM with pixels that can be individually placed in a superposition state of 0 and π. If the pixels were to be mechanical in nature i.e. minute cantilevers, this would involve placing an object of many millions of atoms in a superposition state. However anti-intuitive this may appear, work has been recently reported that suggests this may indeed be possible[16,17]. Even if possible, such a device would not be at all easy to use, having to be operated at cryogenic temperatures to avoid decoherence due to thermal effects.

In the following section an example of how the quantum optical processor may be applied to a well-known decryption problem is described.

4. QUANTUM OPTICAL PROCESSOR FOR A DECRYPTION TASK

As an example of how such a qubit SLM based coherent optical processor could be employed, we apply it to the task of decrypting an image that has been encrypted by applying random phase masks in the image and Fourier plane of the 4-f optical arrangement shown in Figure 1[15]. This converts an input image into a white noise like signal in the output plane. The image is recovered by Fourier transforming the encrypted image, applying a phase mask conjugate to the Fourier plane phase mask and Fourier transforming again to reconstruct the image (which will be complex due to the original image plane phase mask but the original image intensity distribution can easily be obtained by applying a modulus operation to the image data). Thus it is not possible to recover the image from the encrypted output plane signal without knowledge of the Fourier plane phase mask.

We wish to use this method as an example of how a quantum coherent processor could potentially be employed to allow recovery of the image from its encrypted data. We simplify the arrangement slightly in that we assume that the Fourier plane phase mask has only two possible phase values, i.e. 0 or π, to allow the qubit based SLM to match the values. The problem we propose a method of solving with the quantum processor is to determine which one of a known series of images is contained in a given encrypted data array. This restriction will allow us to employ a correlation between each of the known images and the encrypted image to determine which image it is. The encrypted image can not be directly measured from the superposition state generated by the quantum optical processor since any measurement involves a collapse of the wavefunction. In a manner similar to the method employed in the Shor algorithm, the wavefunction must be manipulated so a useful measurement can be made upon its collapse. Thus the most straightforward way of determining which image is encrypted cannot be employed. In an conventional 4-f optical system, the encrypted image could be placed at the input plane, Fourier transformed to the spatial frequency plane and, if the encryption phase code was known, the phase conjugate of this could be placed directly behind the spectrum so formed. This would cancel the phase perturbation and so further Fourier transformation to the output plane intensity detector array would result in reconstruction of the encrypted image. If the phase code was incorrect, a noise-like distribution would be produced instead and the reconstruction fail. Thus successful reconstruction of the encrypted image requires knowledge of the phase code used in the encryption stage, of which there will be 2^N binary phase codes possible for an N pixel binary phase array (and many more for a phase array with more phase levels per pixel). Thus the phase array is effectively a key to secure the encrypted image, knowledge of which is required for decryption of the image. If the key is not known, an exponentially large number of searches must be performed to arrive at the correct phase code and successfully reconstruct the encrypted image.

However, as stated above, we simplify the problem slightly to assume the encrypted image is one of a known set. This could be quite large since we can search the set rapidly with the optical processor. We test each image in turn by placing the image in the input plane and optically Fourier transforming it the spatial frequency plane of the 4-f optical processor. (Additionally, we rotate the input image by 180 degrees in order that its spectrum will be rotated by this angle as well and result in a correlation operation being performed by the processor, rather than a convolution). In the spatial frequency plane we store the phase encoded Fourier spectrum of the encrypted image. Direct Fourier transformation of the spatial frequency plane would result in a noise-like output distribution since the phase code present in the frequency plane will disrupt the signal. However, if we place an SLM in the frequency plane directly behind the plane in which the encrypted image spectrum is stored and place on this the conjugate phase of the encryption phase array, when the input image is the same as the encrypted image, a strong on-axis auto-correlation signal will be generated at the output plane, indicating the correct image is in the input plane. If the image is incorrect, cross-correlation signal will be generated which will not be sharply peaked on-axis.

The problem is that we do not know the phase code to place on the SLM and searching for this would take an exponentially long time with conventional methods. Instead, we place an SLM in the Fourier plane with each pixel in a superposition state to form N qubits (i.e. each in a superposition state of 0 and π). When the correct image is placed at the input plane it will be Fourier transformed and the field emerging from the stored spatial frequency spectrum of the encrypted image will have a residual phase due solely to the encryption phase mask since the phase of the input image Fourier spectrum will have been negated by the matched filter (as the input image matches the encrypted image).

The essential part of this arrangement is shown in Figure 2 which schematically shows the SLM with pixels held in binary superposition states and the interaction of these with the wavefunction propagating through the optics. In this schematic a phase modulated wavefunction is shown, the matched filter correctly having nulled the phase of the input image spectrum but the unknown phase code remaining. In a conventional processor, this residual phase perturbation of the wavefront would disrupt the correlation unless it too was nulled by a correct conjugate phase code i.e. the decryption phase key. However, in the proposed quantum system, the wavefunction propagates through the SLM qubit plane. The SLM generates a superposition of a 0 and π shifted wavefunction at each qubit location, so creating a superposition of 2^N states. One of these will be matched exactly to the unknown phase key, since all combinations of binary phase are generated. Wavefunctions not matched to the phase key will have phase modulations and when Fourier transformed by the lens will not be tightly focussed. However, the wavefunction resulting from the matched phase key will be plane in phase. After passing through the converging lens this will focus to a strongly localised wavefunction on the output detector thus maximising its probability of collapse onto the central pixel in the output photodetector array.

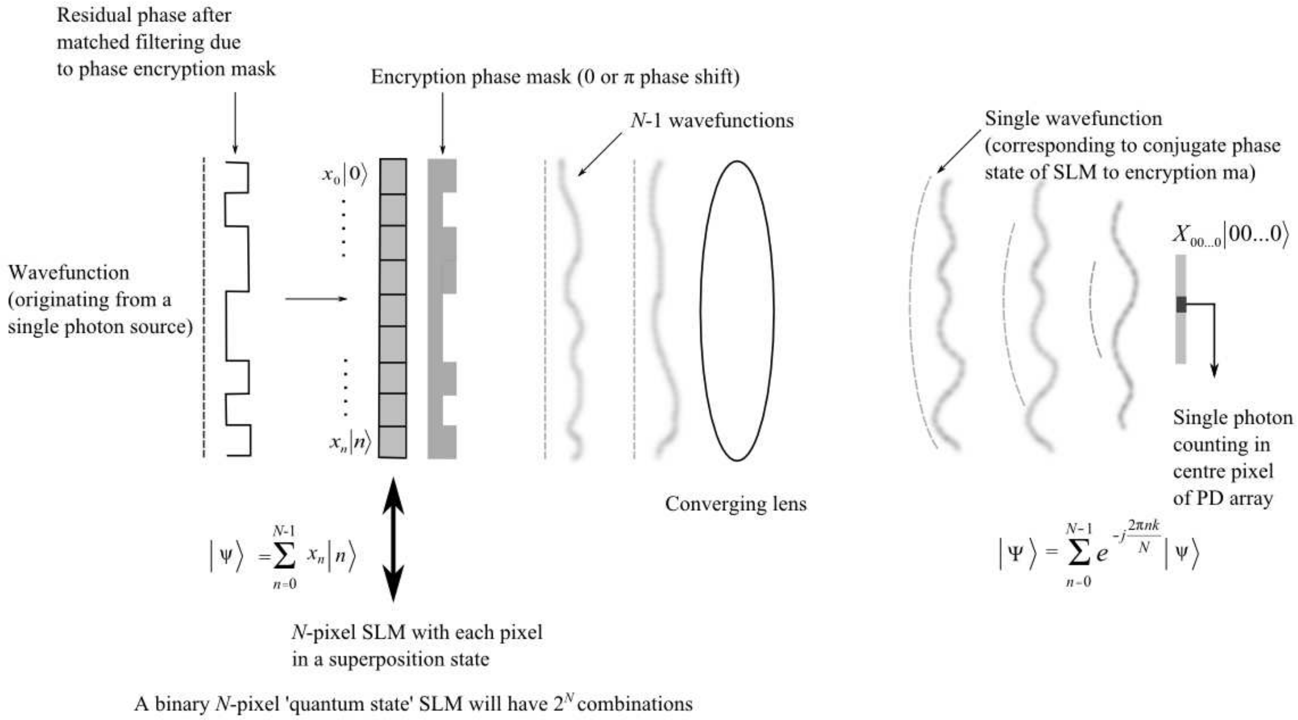

Figure 2. Schematic representation of the superposition states generated by an interaction-free measurement of the SLM pixel qubits propagating through an optical system

As depicted in Figure 2, a single photon at a time is introduced into the optical processor and a measurement of the wavefunction at the output made. This measurement would have to be repeated many times since most photons will be scattered or absorbed, but over many measurements the probability of detecting a photon will be greatest where the wavefunction is concentrated on-axis when a correct input image is present. If the image is incorrect, a residual phase from the matched filter will be present, in addition to that from the phase key, which will not be nulled and so a strong correlation peak will not be generated at the output. Although shown with a single photon in the processor per trial, the considerations noted above in Section 3 may possibly permit the quantum effects to occur with fully coherent faint classical wavefronts, so relaxing the requirements for a single photon source and photon counting detector.

5. CONCLUSION

This paper has described various optical processor configurations based around the classical 4-f coherent optical processor arrangement and considered the possibilities for implementing quantum algorithms with coherent optical processing methods. Suggestions have been made in the literature for implementing the Grover algorithm with 4-f optical configurations. We have shown how a parallel data search can be effectively implemented by a classical coherent optical correlator matched filtering arrangement. However, all the coherent optical implementations of the Grover algorithm operate on a conventional, i.e. non-quantum, memory and so there are physical limitations to how much data can be processed in parallel and the exponential increase in processing power promised by a quantum computer cannot be realised. The Grover algorithm itself, however, does not involve entanglement of quantum bits which is why it can be implemented by a classical optical processor. The Shor quantum factoring algorithm, however, does require qubit entanglement for its implementation and so cannot be realised by a conventional coherent optical processor. Optical processors to implement the Shor algorithm thus require entanglement of the processing photons but this has proved very difficult to achieve for more than a handful of photons thus strictly limiting the size of data input. In this paper, we have proposed placing each pixel of an SLM in a binary superposition state and entangling these by reading out their states with a coherent processing wavefront to provide a so-called interaction-free measurement. In this way, a superposition state of all possible 2^N pixel states of the SLM is created and as the optical wavefunction so generated propagates through the optics of the processor each of the states evolves independently. The unitary operations implemented by the optics of the processor, in particular the Fourier transforming action of a converging lens, thus allow parallel processing of each state. An example of how this exponential increase in processing power may be exploited was given by describing the application of such a system to the solution of a well-known optical encryption problem. Further consideration will in future be given to how the Shor algorithm could be implemented with coherent optical processing configurations employing qubit entanglement on an SLM. If feasible, this would enable the exponential increase in processing power required to solve problems such as large integer factorisation that the Shor algorithm addresses.

REFERENCES

1. Young R., Birch P., Chatwin C., "Coherent optical implementations of the fast Fourier transform and their comparison to the optical implementation of the quantum Fourier transform", Proc SPIE Vol 87480, 874806-1,-11, (2013).
2. Goodman J.W., Introduction to Fourier Optics, McGraw-Hill, Second Edition, (1996).
3. Vander Lugt A., "Signal detection by complex spatial filtering", IEEE Trans. Inform. Theory, Vol. IT-10, pp. 139-145, (1964).
4. Grover L. K., "Quantum computers can search arbitrarily large databases by a single query", Phys. Rev. Lett., Vol. 79, 4709-4712, (1997).
5. Shor P. W., "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer", SIAM J. Comput., Vol. 26(5), pp. 1484-1509, (1997).
6. Hijmans T. W., Huussen T. N., Spreeuw R., J., C., "Time and frequency-domain solutions in an optical analogue of Grover's search algorithm", J. Opt. Soc. Am. B, Vol.24 (2), 214-220, (2007).
7. Bhattacharia N., van Linden H. B., van den Heuvall, Spreeuw R., J. C., "Implementation of quantum search algorithm using classical Fourier optics", Phys. Rev. Lett., Vol. 88, 137901, (2002).
8. Shor P. W., "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer", SIAM J. Comput., Vol. 26(5), pp. 1484-1509, (1997).
9. Ekert A., Jozsa R., "Shor's quantum algorithm for factorizing numbers", Rev. Mod. Phys., Vol. 68, pp. 733-753, (1996).
10. Chuang I. L., Laflamme R., Shor P. W., Zurek W. H., "Quantum computers, factoring and decoherence", Science, Vol. 270, 1633-1635, (1995).
11. Politi, A., Matthews J., O'Brien J., "Shor's factoring algorithm on a photonic chip", Science, Vol. 325, 1221, (2009).
12. Elitzur, A. C., Vaidman, L., "Quantum mechanical interaction-free measurements", Foundations of Physics, Vol. 23, 987-997, (1993).
13. Kwiat P. G., Weinfurter H., Herzog T., Zeillinger A., Kasevich M. A., "Interaction-free measurements", Phys. Rev. Lett., 74(24), 4763, (1995).
14. Kwiat P. G., http://web.archive.org/web/19990222174102/www.p23.lanl.gov/Quantum/kwiat/ifm-folder/ifmtext.html, Accessed: January 2016.
15. Refregier P., Javidi B., "Optical image encryption based on input plane and Fourier plane random encoding", Opt. Lett., Vol. 20(7), 767-769, (1995).
16. Marshall, W., Simon, C., Penrose R., Bouwmeester D., "Towards quantum superposition of a mirror", Phys. Rev. Lett., Vol. 91(13), 130401-1, -4, (2003).
17. Gaidarzhy A., Zolfagharkhani, G., Badzey R. L., Mohanty P., "Evidence for quantized displacement in macroscopic nanomechanical oscillators", Phys. Rev. Lett., Vol. 94(3), 030402-1, -4, (2005).