Imaging and Radiation Research (2023) Volume 6 Issue 1
doi: 10.24294/irr.v6i1.3852

ORIGINAL RESEARCH ARTICLE

Innovative frontiers: Post-quantum perspectives in healthcare and medical imaging

David Josef Herzog[1], Nitsa Judith Herzog[2,*]

[1] *University Fernando Pessoa, Porto 4200-029, Portugal*

[2] *Northumbria University London, London E1 7HT, UK*

*** Corresponding author:** Nitsa Judith Herzog, nitsa.herzog@northumbria.ac.uk

ABSTRACT

The growth of computer power is crucial for the development of contemporary information technologies. Artificial intelligence is a powerful instrument for every aspect of contemporary science, the economy, and society as a whole. Further growth in computing potential opens new prospects for biomedicine and healthcare. The promising works on quantum computing make it possible to increase computing power exponentially. While conventional computing relies on the formula with 2^n bits, the simplified vision of quantum computer power is 2^N, where N is a number of logical qubits. With thousandfold or more improvements in computing performance, there will be realistic options for quick protein, genes and other organic molecules 3D fold discoveries, empowering pharmaceutics and biomedical research. Personalized blockchain-based healthcare will become a reality. Medical imaging and instant healthcare data analysis will significantly speed up diagnostics and treatment control. Biomedical digital twin usage will give useful tools to any healthcare practitioner, with options for intraoperative AR and VR micro-manipulations. Nanoscale intrabody bots will be instantly customized and AI-controlled. The smart environment will be enriched with multiple sensors and actuators, giving real control of the air, water, food, and physical health factors. All these possibilities are quickly achievable only in the case of realistic quantum computing options. Even with the ability to reach this stage, there will be questions for the stability of post-quantum society: privacy, ethical issues, and quantum computing control uncertainty. General solutions to these queries will give clues for post-quantum healthcare.

Keywords: quantum computing; qubit; post-quantum healthcare; medical imaging; biomedical digital twin; big data; AI

ARTICLE INFO

Received: 27 December 2023
Accepted: 11 January 2024
Available online: 19 February 2024

1. Introduction

Moore's law postulates a tendency to double the density of basic semiconductor devices in microchips once every two years. The law is formulated for CMOS-based devices[1]. Machine Learning and Artificial Intelligence (AI) stimulate the development of GPUs[2]. Today, Moore's law is generalized for computing power, including all types of improvements for efficiency, e.g., hardware, algorithms, and software[3]. There are significant achievements in many scientific and technical areas[4,5]. The enormous growth in potential allowed for the development of sophisticated AI systems, from image recognition to big data analytical tools. Smart homes, driverless cars, Natural Language Processing (NLP), Virtual Reality (VR), Haptic technologies, and other multiple AI applications transform life as we know it[6,7]. Many predictions are made about the future possibilities of information technologies. Alternative computing is usually supposed to be an exotic type, suitable for niche exploitation, but includes quantum computing as one of the options.

However, quantum computing could become a disruptive technology of our age, more powerful than all successful inventions of previous decades. If Moore's empirical law represents minimal exponential growth with factor 2, the increasing capacity of quantum computers is potentially much higher. The superposition of two opposite quantum states, reflected by the poles of the Riemann sphere, is distributed until the wave function collapses. While bit displays binary combinations, qubit represents the probability of all possible states at one time before the observer effect will settle the system. Conventional computing relies on the formula with 2^n bits. The simplified vision of quantum computer power is 2^N, where N is the number of logical qubits. Since the qubit is a matrix of all simultaneously available bit combinations, the potential speed of basic computational operations grows enormously[8]. The universal quantum computer, built from multiple quantum logical gates, has the prospect of significant computational power growth.

Singularity is often seen as a theoretical, hard-to-achieve phenomenon. However, if difficulties in creating effective universal quantum computing with thousands of logical qubits are resolved, it will open numerous opportunities, described as post-singularity[9]. Post-quantum technologies will allow the development of a smart environment, from smart homes and smart cities to smart infrastructure. Industry 4.0 and the Internet of Things will be developed from a cyber-physical state to the level of cyber-biological Industry 5.0. The digital twinning of nature, infrastructure objects, people, and society will be united in one complex, dynamic, interactive reality. For healthcare, it will mean real-time biomedical digital twinning from the atomic and molecular nano-level to tissues, organs, systems, organisms, and societal levels.

The industrial and synthetic biology of the fifth revolution will open opportunities for healthcare applications. Dynamic omics databases will allow serious advances in clinical research and pharmacology[10], medical imaging and smart laboratories will give keys to immediate diagnostics and personalized effective treatment, blockchain research and electronic medical records will unite individual measures and public health arrangements. Training opportunities will be supported by VR-situated tasks with haptic tools enabled. Clinical practice will be enhanced by ubiquitous Augmented Reality (AR) devices, creating Mixed Reality (MR). Robotic surgery will achieve a much more sophisticated level with routine automatic replacement of microscopic, very difficult, and repetitive functions by machine-controlled support. Diagnostic automatic support and Ambient Assisted Living (AAL)[11] will help reduce the financial burden of healthcare and spread it to rural and less developed areas.

All these changes will be possible with the ability to drastically reduce noise in universal quantum computing systems with thousands of manageable logical qubits[12]. Specialized quantum computing systems allow thousands of physical qubits, but this is still short of quantum advantage and does not make classical computing redundant. The quantum coherence, which makes qubits effectively larger than a bit, with a spectrum of superposition values from 0 to 1, is susceptible to noise from external sources. Preserving a high number of quantum mechanical states, protected from external "non-quantum" and "observed" states, is a difficult task that has not yet been fully solved. There are propositions for de-noising the quantum system, protective techniques, and parallel computing approaches to multiple quantum gates. The question is still widely debatable on a theoretical level. All this makes post-quantum healthcare a matter of hypothetical predictions, depending on the probability of practical realizations. Powerful classical computing may help to achieve a state equal to quantum advantage in the distant future. For the article's structure, address **Figure 1** below.

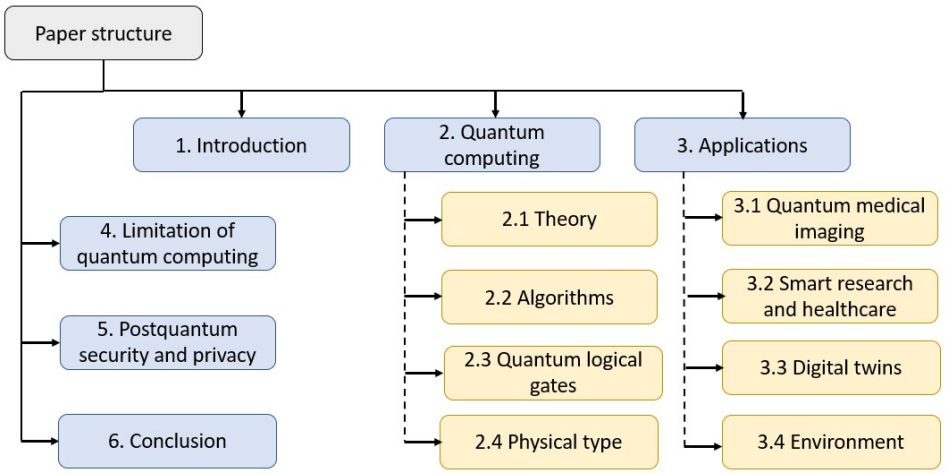


Figure 1. Roadmap of the article.

2. Quantum computing

Atomic and quantum effects studies, developing from the end of the nineteenth century, led to the formulation of quantum mechanics. Heisenberg uncertainty principle and Schroedinger's equation formulated the unique property of quanta—dualistic nature, which allows the interposition of states, impossible in classical mechanics. Quantum informatics was developed in the 60s and 70s by Gordon, James Park, and others. In 1973, Holevo[13] made proof for the upper bound of quantum information transmission[8]. The idea of the possibility of exploiting quantum effects for computing devices was stated by Bernioff in 1980[8]. At the same time, Shor[14] proposed a mathematical model for quantum computing. Richard Feynman limited the possibility of successfully imitating quantum processes only in quantum computers[15]. David Deutsch, in 1985, postulated the possibility of creating a universal quantum computer, which could have properties of a unique Turing machine with quantum parallelism[16]. Quantum algorithms were proposed in 1990th by Shor[14], Deutsch[17] and others, while Abstract State Machine (ASM) was formulated in 1980th by Gurevich[18]. According to him, any ASM can be reproduced physically by the gradual implementation of steps from a theoretical algorithm. Quantum computing is developing in many ways, according to the chosen quantum medium, but remains in the early stages. However, there are proposals to see the Universe as a sort of quantum computer by itself, not just a universal Turing machine.

2.1. Theory

Quantum dualism is described by the equation derived from the De Broglie wave function hypothesis[19]. Quantum mechanics is generally formulated by the Schroedinger equation, where the wave function is represented by complex numbers in Hilbert space[12]. The matrix equivalent was proposed by Werner Heisenberg[20]. Quantum states are represented by a superposition of probabilities' densities. The wave function "collapses" during measurement or observation time into a classical state. The two qubits, for example, will be a superposition of four potential bits, which will become classical bits in the moment of observation. However, if computation is done in a quantum state, in the moment of observation, quantum parallelism will produce a significant speed-up of the system. The quantum computing system is usually built from quantum logic gates as unitary operators, able to perform classical Boolean binary operations AND, OR, NOT, with the unique property of reverse[12].

Single qubits can be graphically depicted by the Bloch sphere, n-sphere, where $n = 2$ (see **Figure 2**). The opposite poles of the sphere, $|1\rangle$ and $|0\rangle$, are orthogonal quantum state vectors (). The point $|\psi\rangle$ on the surface of the sphere, pure quantum state, shows the projection of internal superposition quantum states, where Θ and

φ are angles in the sphere coordinates. The dynamic of quantum states can be reflected by Bloch sphere rotation. Qubits and qutrits represent higher superposition states and cannot be demonstrated on the Bloch sphere[21].

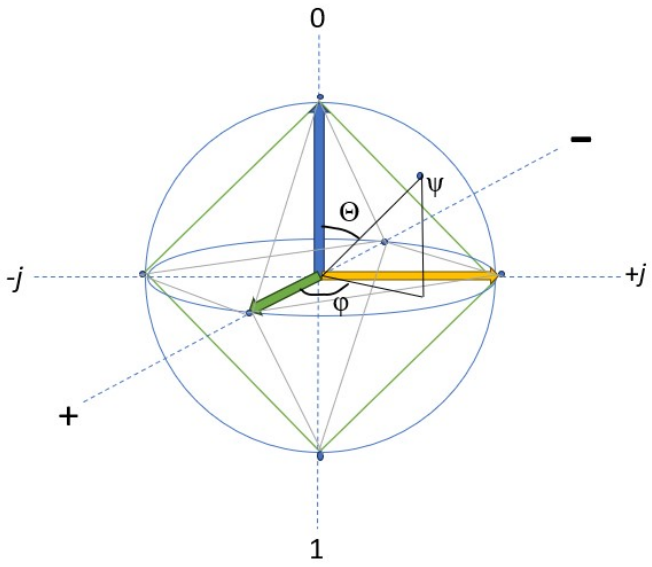


Figure 2. Bloch sphere.

2.2. Algorithms

Gurevich worked in 1980th on the finite model theory and developed algebras for Abstract State Machines and the generalization of Finite State Machines[18]. The Universal Turing Machine, according to ASM, can replicate any algorithm. One of the postulates of ASM theory bridges theoretical algorithms with practical implementation. Quantum algorithms, then, show the possibility for the gradual physical embodiment of a universal quantum computer or quantum Turing Machine. Today, there are more than two hundred quantum algorithms suitable for different computing tasks.

Deutsch–Jozsa algorithm, developed by Deutsch in 1985 (the full version was published in 1992) is designed for search strategy[17]. It uses a binary approach to separate between two types of functions. The Deutsch–Jozsa algorithm showed exponentially better computing time than classical algorithms. The other well-known quantum algorithm with a time shorter than any non-quantum algorithm and development of the Deutsch–Jozsa algorithm, was proposed by Bernstein and Vazirani in 1992[22].

In 1994, the factoring quantum algorithm was proposed by Shor[14]. Factorization is the basis of public-key cryptography. Deterministic machines run factoring algorithms in more than polynomial time and less than exponential. Shor's algorithm runs in polynomial time and is exponential, which gives a potential advantage in the case of powerful quantum machine utilization. However, it does not solve the P/NP problem. Shor's algorithm consists of quantum and classical computing parts.

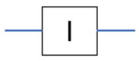
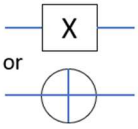
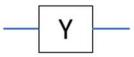
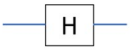
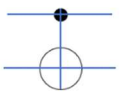
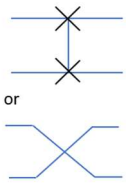
Non-exponential algorithms, proposed in 1996 by Grover, take minimal time to search unsorted data if compared with other algorithms[23]. The exponent advantage over other search algorithms equals two, but Grover's algorithm is still close to the optimal time for a non-deterministic Turing Machine. Despite the relatively slow speed up in comparison with other quantum algorithms, Grover's algorithm is recognized as problematic for classical cryptography.

2.3. Quantum logical gates

A Quantum computing device is usually built from the combinations of quantum logical gates or quantum circuits. The quantum gates are devised to handle standard logical operations. A Quantum gate is associated

with a certain operational algorithm. The power of the gate is from one to a few qubits. The longest pass in the quantum circuit defines quantum depth. Operations of the quantum gate are described by unitary or orthonormal square matrix, where vectors are reflected by complex or real numbers in rows and columns. NOT gate is one qubit, four positions in the 2 × 2 matrix, reflected by operations in the direction of the X-axis in the Bloch sphere, defined by the angle phi. Other gate names are Pauli X, Pauli Z, and Pauli Y, which are gates with matrix numbers related to the named axes. Pauli I, X, Z and Y gates are described by the related Pauli matrix[24] (see **Table 1**).

Table 1. Basic quantum gates and their properties.

Quantum gate	Circuit diagram	Matrix	Equation
Pauli-I (Identity)		$\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}$	$I = \|0\rangle\langle 0\|+\|1\rangle\langle 1\|$
Pauli-X (or NOT)		$\begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}$	$X = \|0\rangle\langle 1\|+\|1\rangle\langle 0\|$
Pauli-Y		$\begin{bmatrix}0 & i\\i & 0\end{bmatrix}$	$Y = \|0\rangle\langle i\|+\|-i\rangle\langle 0\|$
Pauli-Z		$\begin{bmatrix}1 & 0\\0 & -1\end{bmatrix}$	$Z = \|0\rangle\langle 0\|+\|1\rangle\langle -1\|$
Hadamard		$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}$	$H = \frac{\|0\rangle+\|1\rangle}{\sqrt{2}}\langle 0\| + \frac{\|0\rangle-\|1\rangle}{\sqrt{2}}\langle 1\|$
CNOT		$\begin{bmatrix}1 & 0 & 0 & 0\\0 & 1 & 0 & 0\\0 & 0 & 0 & 1\\0 & 0 & 1 & 0\end{bmatrix}$	$CNOT = \|0\rangle\langle 0\| \otimes I + \|1\rangle\langle 1\| \otimes X$
SWAP		$\begin{bmatrix}1 & 0 & 0 & 0\\0 & 0 & 1 & 0\\0 & 1 & 0 & 0\\0 & 0 & 0 & 1\end{bmatrix}$	$SWAP = \|00\rangle\langle 00\| + \|01\rangle\langle 10\| + \|10\rangle\langle 01\| + \|11\rangle\langle 11\|$

CNOT, Controlled NOT gate, requires the matrix of at least 2 qubits or a minimum 4 × 4 matrix[14]. It has the properties of a classical XOR gate but with the option of reversible operability. Controlled Z and Y gates also have 2 or more qubit potential. Hadamard is the single-qubit gate, where the sum of $|1\rangle$ and $|0\rangle$ is divided by the square root of two, showing the superposition of quanta. As a result, it gives 0 or 1 around 50% of the time in each case, with correction for error. The Hadamard matrix represents it. Swap gate two qubits gate, 4 × 4 matrix. It allows swapping operations between two qubits. Mathematically, all named above gates are Clifford type, where possible operations in the so-called Clifford group are described in Gottesman–Knill theorem. Clifford gates are suitable for efficient simulation on classical computers. Other, non-Clifford gates, require more resources for implementation and simulation but are more powerful.

Toffoli gate, in other words, a Controlled CNOT 8 × 8 matrix, the same as a Fredkin gate, represents Controlled SWAP[25]. There are more variations: square root NOT, square root SWAP, and square root CNOT gate representation. Universal quantum gates can be transformed between each other. Deutsch gate is theoretical, without an associated algorithm.

2.4. Physical types

The quantum mechanical states can be utilized for computing in different ways. Several physical ways of implementing systems based on quantum effects are proposed for computing devices. The fundamental principle is to use a coherent pair of "quanta" connected by some sort of quantum interdependence[12]. This pair has a superposition of quantum states, opening the way for the logical quantum gate operation. A combination of logical gates, often parallel with the option of scalability, is the core of the quantum computer. The decoherence time and speed of the quantum gate are important for the functioning of quantum gate computers. There are other models of quantum computers based on quantum annealing or topological anyone pairs.

DiVincenzo formulated several principles for a successful quantum computing system[26]. The first one is a scalable physical system with well-characterized qubits. A well-characterized qubit has several requirements: coupling with other states of a qubit, interaction with other qubits, and well-known physical parameters. The second one is the ability to initialize the state of the qubits to a simple, fiducial, detectable state. The computation must start from a well-known value for obtaining results and error correction. The third principle requires long decoherence times compared to the gate operational time. Decoherence time must be much longer to allow successful computation with minimal possible error. The fourth principle is a universal set of quantum gates. The fifth principle requires qubit-specific measurement capability, which includes a rerun of measurement in the case of a higher probability of results in the case of repeated calculations.

Several physical systems meet DiVincenzo's requirements. In Nuclear Magnetic Resonance (NMR), quantum computers operate on the principle of spin difference between molecules with a non-whole spin of n + ½, fermions, where n is a natural number and whole number spin molecular environment of bosons. The important part of the technique is the controlled quantum state, so crystal solid-state magnetic resonance quantum computers. Low-temperature superconducting makes possible changes in the behavior of nuclei or electrons with partial spin numbers into full spin numbers or bosons, creating Bose-Einstein condensate. Cooper's pair of fermions are not subject to the Pauli exclusion principle at temperatures below Fermi's temperature for the system. Electron Spin Resonance (ESR) electron spin system, based on coupled fermions, also allows quantum computing. **Figure 3** demonstrates an example of a quantum computer used by IBM.

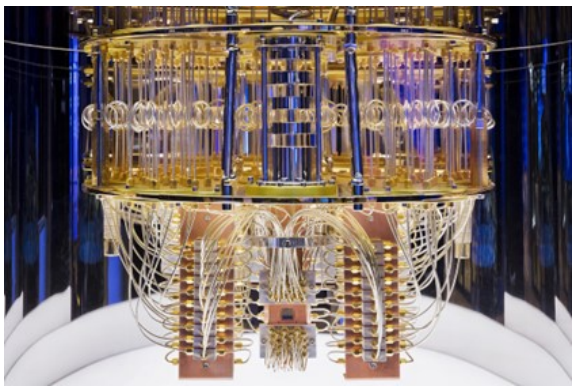


Figure 3. Flickr: IBM Quantum System One (CES 2020). Interior of an IBM Quantum computing system. (Credit: IBM, license: CC BY-ND 2.0 – allows to share - copy and redistribute the material in any medium or format for any purpose, even commercially).

There are other systems, such as quantum dot manipulation of an external electron in the ion by laser energy source. Quantum dots are usually nanoparticles, included in semi-conductive material and behave in accordance with quantum mechanical rules when excited. The other type of quantum computer, optical quantum computers, is based on different states of paired photons[21] or the interaction of photons with atoms and molecules. Diamond-based, nitrogen-vacant (NV) quantum computers are also possible[27]. Diamonds provide the possibility for the system to operate at room temperature. Quantum well computers also can

function at room temperature. There are more systemic principles, such as charged ions, trapped ions[28], molecular magnets and many others.

3. Applications

There is constant progress in the field. Quantum computing devices are actively researched, evolving towards more complex forms with a higher number of qubits. Potential applications involve all areas of robust computing. Big Data analysis and control, AI, Digital Twinning, Smart environment, VR and AR applied in healthcare are at the forefront of practical planning. Clinical research and practice will have significant advantages, being empowered by the exponential growth of computer power. **Figure 4** shows the application areas of quantum computing.

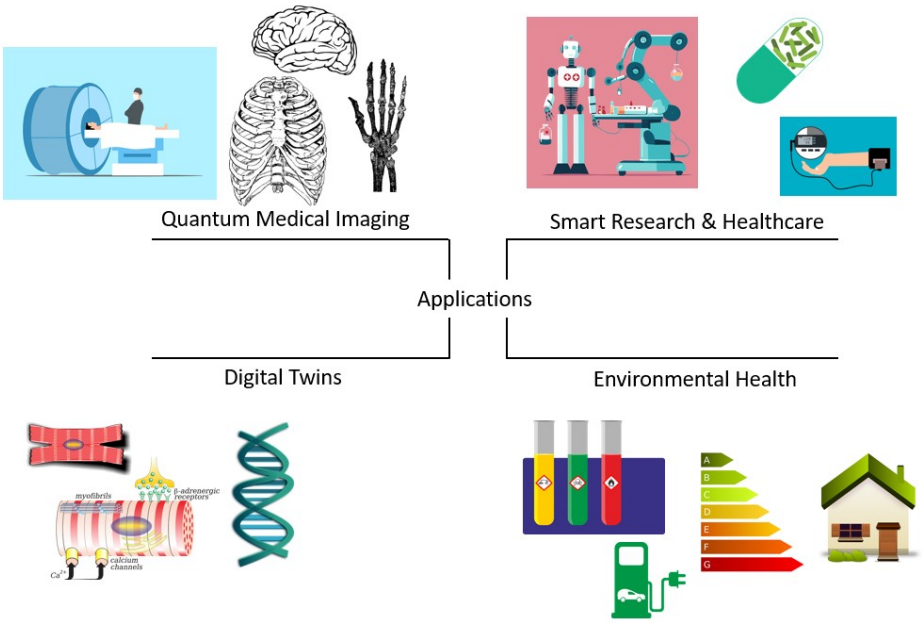


Figure 4. Healthcare applications that can utilize AI and quantum computing.

3.1. Quantum medical imaging

Medical imaging is one of the main applications of AI and Deep Learning in contemporary healthcare. Classical medical imaging is supposed to be a result of X-ray, Computer Tomography (CT), Ultrasound (US) and Magnetic Resonance Imaging (MRI) diagnosis methods, including volumetric analysis. The public is usually captivated by neuroimaging, while real success is seen in many areas, from US live echocardiology and functional and molecular MRI[29] to ophthalmic fundoscopy, Positron Emission Tomography (PET) and micro-histologic imaging. AI and machine learning (ML) techniques are remarkably successful in these areas and enable quick, efficient and frequent diagnostic support[30]. Medical imaging or any laboratory methods cannot be the single source of diagnosis. Medical diagnosis is a result of professional judgment based on several facets, from complaints to sophisticated medical investigations[31].

The contemporary AI approach makes imaging methods not only more precise and widespread but also more universally used[32]. It opens possibilities for instant in-operation video-streaming analysis for endoscopic surgery, immediate histology analysis for intraoperative biopsy, and speedy immune analysis of blood, other bodily fluids, and tissues. Rapid comparative analysis allows fast pre-diagnostic tests for skin conditions, even for unprofessionally made pictures. Quantum computing possibilities determine these options as more robust, swift, and ubiquitous. There is a potential for a black box solution which currently limits AI use in medicine for medical legal and practical reasons.

Medical imaging includes several steps. Image acquisition is followed by image transformation, feature analysis, modelling and image data handling. Specific quantum techniques and algorithms are proposed for different stages of medical imaging (see **Figure 5**). While images obtained with the help of classical methods can be analyzed by quantum techniques, there are also unique approaches in quantum imaging. Ghost imaging (not to be confused with ghost imaging in MRI) shortens patients' exposure, helps obtain information from scarce data, and provides an opportunity for speeding up the process due to the direct transfer of quantum data to Quantum Processing Unite (QPU). Quantum Dots (QD) allow precise radio, immunologic and biochemical labelling[33]. It can be effective as a contrast for quantum MRI and used for theranostics when labelled tissue is treated by targeting nanoparticles.

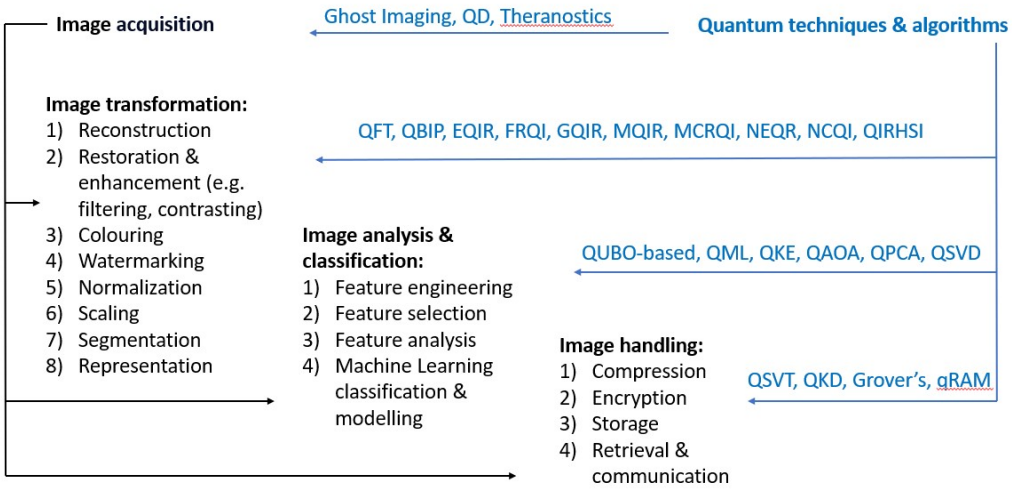


Figure 5. Quantum medical imaging, algorithms and techniques.

Multiple algorithms are proposed for image transformation. A large part of them is focused on quantum image representation, such as Enhanced Quantum Image Representation (EQIR), General Quantum Image Representation (GQIR), Multimode Quantum Image Representation (MQIR), Novel Colour Image representation (NCQI), Multichannel Representation for Quantum Imaging (MCRQI), Novel Enhanced Quantum Representation (NEQR), and Quantum Image Representation based on HSI colour space (QIRHSI). Direct and inverse transform techniques are represented by the Quantum Fourier Transform algorithm (QFT)[30]. Quantum Image Boolean Processing (QBIP) enhances images through denoising.

Feature engineering can be done by Quadratic Unconstrained Binary Optimization (QUBO)-based quantum algorithms[34], Quantum Approximate Optimization Algorithm (QAOA), Quantum Principal Component Analysis (QPCA), and Quantum Singular Vector Decomposition (QSVD). Quantum ML is also represented by the Quantum Kernel Estimation (QKE) algorithm. Quantum image handling includes Quantum Singular Value Transformation (QSVT), Quantum Key Distribution (QKD), the algorithm used for data encryption and Grove's algorithm for data retrieval[30]. Specialized quantum Rapid Access Memory (qRAM) is proposed for efficient data handling.

Biomedical digital twinning goes beyond standard biomedical imaging or simulations. Personal genome, proteome, microbiome, and neuroconnectome[35], together with working 3D twins of organs, systems, and the whole body, became possible[36]. Significant processing power growth will help handle information streams from biomedical objects to the twin and back. It will allow further automatization of diagnostic and treatment procedures through the changes first applied in a twin itself. Powerful quantum servers can deliver solutions for telemedicine literally across the globe, handling a constant flow of diagnosis still images, videos, and other

biomedical information. It can easily combine several sources of information to propose complex pre-diagnostic support not only for healthcare professionals but also for ordinary patients.

The same area of quantum computing poses a significant challenge for streaming sensitive medical information. Besides standard data protection and cybersecurity methods, some other techniques have been proposed for the post-quantum era.

3.2. Smart research and healthcare

Highly effective AI, united with multiple databases and platforms, can empower clinical research. Quantum computing is able to add several levels of productivity. Full genome analysis can be quick and personalized, with the ability to single out productive sites and their control, epigenetic regulation. Besides individual clinical maps of every potential patient, it is possible to pinpoint medication sensitivity and effectiveness in every case. Full-fledged experiments in silico will help target specific genome areas for wide research[29]. New medications, individualized treatments, and quick diagnostics of genetic diseases with the possibility of effective genetic engineering would be achievable at this level.

It will be possible to reproduce and control all transcription and translation processes, including post-translational modifications, and quickly and easily reproduce genetic code from proteins. 3D protein folding will be solved without extensive and time-consuming laboratory efforts, changing pharmacology, immunology, and clinical medicine[37]. Membrane proteins, receptors, enzymes, hormones, and synaptic regulation will be recreated in silico and potentially reproduced in vitro and in vivo. Metabolomic networks will be visible in real time. On a molecular level, nanobot control will be achievable.

In clinical medicine, multiple tools will be available under the control of AI used by quantum computer[29]. The brain-computer interface will receive robust updates, with a strong bidirectional effective communication channel. Implanted functional and data connective chips will be controlled from the cloud. Full modular 3D models on the organismic level, from the molecular and cellular levels, for every area will be part of the healthcare records. The universal healthcare records will be easy to update in time, and they will contain all necessary information, including video analysis, blockchain of events and recommendations, updated by recent clinical research. An immediate diagnosis and treatment recommendations with the help of diagnostic software will relieve the queue for the specialists' consultation, the bottleneck in the emergency and first help.

The application of special diagnostic tools and methods of quick laboratory solutions, MRI and US medical imaging analysis through the universal cloud applications will drastically speed up the process. The task flow control and healthcare management will distribute resources efficiently. VR applications with haptic technologies will provide an immersive environment for students. AR will be widely applied even in routine medical checks. Robotic surgery will be enhanced with tools, allowing sophisticated treatment. AAL will produce electronic health records and contact services automatically in case of an emergency[11]. Hybrid quantum-classical computing, where single-board Tensor Processing Units (TPU) provide Edge computing[7] and quantum AI is on the server side, can open a new chapter for AAL and Telemedicine.

3.3. Digital twins

The digital twin concept was created as a part of the product lifecycle control. With time, it developed into the multilevel digitalization of material objects. Healthcare is an important field for the development of the digital twin concept[10]. It has applications in genomics, proteomics, and metabolomics and is used in clinical research in silico and modelling. Cyber-physical simulations are actively used in medical education and healthcare management. The concept of the Internet of Medical Things (IoMT) is widened to the Internet of Bio-Nano Things (IoBNT). Where exists permanent data flow between bio-physical objects and digital twin siblings.

Customization, virtual, and augmented reality with support by 3D digital twins is a step towards Industry 5.0. The constant communication of human operators with Industry 4.0 infrastructure plus biomedical digital twinning will make it. The concept of Industry 5.0 is based on bio-printing, VR, AR and holograms as part of operational dynamic control of biomedical objects and environment through the digital twins. Moreover, it is the general point of cyber-biological space and its interactions. Cyber-biological systems potentially range from biosensors and DNA programming to the multiscale biosensing and interactive Digital Twin of the biosphere[34].

The goal is to present an object, process or environment as a data aggregate. The levels go up from the atomic and molecular to population and the biophysical world[38]. Digital twins can be structural, physiological, behavioural and complex[39]. These types of digital twins, made for the same biological object with different functionality, are called digital siblings. The higher levels are often presented as modular when interaction with other twins and the environment are included.

3.4. Environment

One of the widest potential applications of quantum computing is smart infrastructure and a smart environment. A smart environment with ongoing control of the air, water and soil quality, supplemented by drinking water and indoor self-regulated ventilation, can significantly improve quality of life and sustainability. There is a well-known dependence of the population's health and life expectancy on environmental factors. Pollution prevention and sanitary and hygienic control with the help of multiple sensors and actuators will improve all aspects of everyday life. Systemic observation of the environment and prediction of potential sources of great disruptions, such as volcanic eruptions, earthquakes, tsunamis, hurricanes, and floods, requires not only highly effective predictive models for AI but also global networks of controlling points for data acquisition. Rivers' flow, reservoirs, and dam conditions have to be supervised. More exotic dangers of extraterrestrial radiation, asteroids, and real ones of falling artificial satellites and rocket parts also need permanent control of multiple factors and objects. Space debris, natural and artificial, has already become a potential source of disruption through satellite damage.

Quantum AI public can be applied to public health trends analysis[40]. It is required for quick reaction and disaster management in the case of epidemics, catastrophes, and social and military conflicts. Environmental control includes toxic waste control and virtual inspections with the help of smart operative tools. Radioactive element pollution and radiation observation require multiple observation points united into networks. Soil, air, and water pollution is often caused by biological waste, microbial, fungal or viral materials[41]. There is a necessity to check the quality of sources and territories, which can be effectively enabled only with the help of powerful networks with AI computing units. Control must be done with multiple sensors, reporting computers and analytical nodes. The operative abilities of quantum computing make this approach achievable.

4. Limitation of quantum computing

Quantum computing is developing fast, but it may have fundamental limitations. Some experts have expressed diverse opinions about the future of quantum computing systems. While there is significant success in quantum systems created for specific tasks, universal computing is claimed to be hard to reach. Quantum states theory reflects the necessity to consider the probabilistic nature of quantum measurement. While for small-scale systems of few qubits, error produced by the noise can be successfully dealt with, for systems of 50–100 qubits, necessary Noisy Intermediate-Scale Quantum Algorithms (NISQ) are required[12]. The de-noising practice will take significant resources on a bigger scale of thousands and more qubits. According to some assumptions, more than 99% of computer power will be spent on error correction[28]. Together with the resources required for the reversible quantum gates, they will reduce the abilities of any quantum computing

system to a low level, which is insufficient for quantum advantage. In accordance with the threshold theorem, the Fault-Tolerant Quantum Computation (FTQC) is possible[26]. However, highly entangled states are not met in nature and require error correction in the quantum control code, which is not free from potential contradictions, e.g., conflicting parts. In addition to the error correction methods mentioned earlier (gate error correction, error correction algorithms, decoherence error correction), there are other techniques to tackle the problem: real-time error monitoring, hybrid quantum-classical external error correction blocks and general denoising depending on the physical principals used in quantum computing systems.

The time of decoherence is crucial for a quantum computing system, and for big systems, it critically depends on the temperature with a low possibility of successful implementation. The powerful quantum system will require control of 10^{300} quantum states simultaneously, which is impossible. There are 10^{80} particles of matter in the observed Universe and 10^{90} photons and neutrinos, which makes all information 10^{122} bits, including gravitational degrees of freedom. Even 400 simultaneously entangled particles will exceed the informational level of the Universe. When there is a necessity to entangle at least thousands of particles for successful quantum computing, the task contradicts the holographic principle postulated in string theory. Hence, it is not sufficient to compare the complexity of quantum states only with Hilbert space dimensionality.

There are other theoretical problems which are seen as fundamental obstacles to quantum computing. An optimistic view claims that the quantum computing system will clarify the P/NP problem[42]. But it might be impossible even for a supreme computing system. The other hypothesis claims the creation of AI + machines by AI machines, while the next generation will be AI++ machines[9]. At this stage, any computational system will become more effective and autonomous, if not conscious in traditional terms, than humans. Hence, quantum computers are dangerous to use in terms of quantum advantage and as devices with potential above anything humankind has experienced before. However, the Kolmogorov complexity principle puts a limit on it[43]. Can a less complex algorithm be written to control a more complex one? It can be re-stated in terms of equality of algorithm and device to run it: is it possible to create a complex machine by a less complex one?

5. Post-quantum security and privacy

Post-quantum healthcare will have advantages and complications connected to the unique abilities of quantum computing. Quantum algorithms and computer power will break any security based on pre-quantum algorithms[44]. Personal healthcare records are a source of highly sensitive information. If privacy protection is removed, social and other outcomes will be serious enough to disrupt “normal” life as we know it. At the same time, the quantity of personal information will grow exponentially. Together with ineffective security, it will expose not only the personal level of information but also governmental, organizational, and societal information to unwanted recipients.

Grover’s algorithm can help solve lower numbers of symmetric key cryptography. The current level is below Grover 128. Shor’s algorithm in the quantum computer of several thousand qubits can solve the RSA code of any practical length, similar to DSA. The same applies to public key elliptic curve cryptography (ECC)[44]. Lattice-based cryptography is one of the solutions. LBC is based on applying the Learning with Errors (LWE) computational problem. Hash functions cryptography also can be based on the lattice. A hash function maps strings of arbitrary size to strings of fixed length. There are several other crypto-resistant algorithms and methods: code-based cryptography (CBC), Multivariate Cryptography (MVC), and Isogeny-Based Cryptography (IBC)[45].

Classical cryptography must be phased out in the wake of quantum algorithms applications on quantum computing devices. However, significant areas of records and networks are protected by pre-quantum methods. It will require massive investment in the area, including equipment, education, and standardization. Work has

been done on the standardization of new methods[43]. Blockchain is one of the methods to strengthen security in the post-quantum era.

6. Conclusion

Abstract state machine principles connect algorithms with the physical possibility of constructing devices based on these algorithms. Quantum computing devices are not only possible in principle but are also becoming more powerful and sophisticated. Currently, quantum computing is still in the early stages of development. There are several areas for potential applications. Smart environments, digital twinning, ubiquitous computing, and universal AI can be significantly enriched by quantum computing or hybrid quantum-classical implementation. The strong advantages are a quantum leap in computational speed, the ability to process much higher data volumes than classical computing, and the possibility to use specific quantum effects to upgrade existing computational mechanisms.

There are several prospective applications of quantum computing in healthcare, from medical imaging to genomics, proteomics, and metabolomics. It opens opportunities for swift healthcare data acquisition, fast medical data collection, effective machine-based diagnostic systems, unitary health records administration, and personalized medical treatment. The robust capacity to process real-time streaming data grants the opportunity to generate highly sophisticated biomedical twins of cells, tissues, organs, and organisms. The computational power of quantum computing can help with VR/AR/MR utilization for professional education and clinical practice, healthcare management, and personalized blockchain records. It is also important to take into account that the wider opportunity brings potential challenges. For instance, it will require enhanced security measures and data awareness. Post-quantum healthcare will certainly necessitate closer collaboration between health professionals and technical specialists.

Author contributions

Conceptualization, DJH and NJH; methodology, DJH; validation, DJH and NJH; formal analysis, DJH; investigation, DJH; resources, DJH; writing—original draft preparation, DJH; writing—review and editing, NJH; visualization, NJH. All authors have read and agreed to the published version of the manuscript.

Conflict of interest

The authors declare that they have no conflict of interest.

References

1. Shalf J. The future of computing beyond Moore's Law. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 2020; 378(2166): 20190061. doi: 10.1098/rsta.2019.0061
2. Wang Y, Zhao Y. Arbitrary spatial trajectory reconstruction based on a single inertial sensor. *IEEE Sensors Journal* 2023; 23(9): 10009–10022. doi: 10.1109/jsen.2023.3257867
3. Leiserson CE, Thompson NC, Emer JS, et al. There's plenty of room at the top: What will drive computer performance after Moore's law? *Science* 2020; 368(6495). doi: 10.1126/science.aam9744
4. Choi S, Yang J, Wang G. Emerging memristive artificial synapses and neurons for energy-efficient neuromorphic computing. *Advanced Materials* 2020; 32(51). doi: 10.1002/adma.202004659
5. Al-Dujaili MJ, Al-dulaimi MA. Fifth-generation telecommunications technologies: Features, architecture, challenges and solutions. *Wireless Personal Communications* 2022; 128(1): 447–469. doi: 10.1007/s11277-022-09962-x
6. Wang Y, Zhao Y. Handwriting recognition under natural writing habits based on a low-cost inertial sensor. *IEEE Sensors Journal* 2024; 24(1): 995–1005. doi: 10.1109/jsen.2023.3331011
7. Zhang J, Tao D. Empowering things with intelligence: A survey of the progress, challenges, and opportunities in artificial intelligence of things. *IEEE Internet of Things Journal* 2021; 8(10): 7789–7817. doi: 10.1109/jiot.2020.3039359
8. Benioff P. The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of

computers as represented by turing machines. *Journal of Statistical Physics* 1980; 22(5): 563–591. doi: 10.1007/bf01011339
9. Chalmers DJ. The singularity: A philosophical analysis. In: *Science Fiction and Philosophy: From Time Travel to Superintelligence*. John Wiley & Sons, Inc.; 2016. pp. 171–224. doi: 10.1002/9781118922590.ch16
10. Fuller A, Fan Z, Day C, et al. Digital twin: Enabling technologies, challenges and open research. *IEEE Access* 2020; 8: 108952–108971. doi: 10.1109/access.2020.2998358
11. Rashidi P, Mihailidis A. A survey on ambient-assisted living tools for older adults. *IEEE Journal of Biomedical and Health Informatics* 2013; 17(3): 579–590. doi: 10.1109/jbhi.2012.2234129
12. Preskill J. Quantum computing in the NISQ era and beyond. *Quantum* 2018; 2: 79. doi: 10.22331/q-2018-08-06-79
13. Holevo AS. Bounds for the quantity of information transmitted by a quantum communication channel. *Problemy Peredachi Informatsii* 1973; 9(3): 3–11.
14. Shor PW. Quantum computing. *Documenta Mathematica* 1998; 1(1000): 467–486.
15. Feynman RP. Simulating physics with computers. *International Journal of Theoretical Physics* 1982; 21(6–7): 467–488. doi: 10.1007/bf02650179
16. Deutsch D. Quantum theory, the Church–Turing principle and the universal quantum computer. *Proceedings of the Royal Society of London A Mathematical and Physical Sciences* 1985; 400(1818): 97–117. doi: 10.1098/rspa.1985.0070
17. Deutsch D, Jozsa R. Rapid solution of problems by quantum computation. *Proceedings of the Royal Society of London Series A: Mathematical and Physical Sciences* 1992; 439(1907): 553–558. doi: 10.1098/rspa.1992.0167
18. Gurevich Y. Logic in computer science column. *Bulletin of the EATCS* 1989; 38: 93–100.
19. De Broglie L. The wave nature of the electron. *Nobel Lecture* 1929; 12: 244–256.
20. Heisenberg W. *The Physical Principles of the Quantum Theory*. Courier Corporation; 1949.
21. Joo J, Knight PL, O'Brien JL, et al. One-way quantum computation with four-dimensional photonic qudits. *Physical Review A* 2007; 76(5). doi: 10.1103/physreva.76.052326
22. Bennett CH, Bernstein E, Brassard G, et al. Strengths and weaknesses of quantum computing. *SIAM Journal on Computing* 1997; 26(5): 1510–1523. doi: 10.1137/s0097539796300933
23. Grover LK. A fast quantum mechanical algorithm for database search. In: Proceedings of the twenty-eighth annual ACM symposium on Theory of computing; 22–24 May 1996; Philadelphia Pennsylvania, USA. pp. 212–219. doi: 10.1145/237814.237866
24. Preskill J. Quantum information. In: Preskill J (editor). *Quantum Shannon Theory*. Cambridge University Press; 2016.
25. Fredkin E, Toffoli T. Conservative logic. *International Journal of Theoretical Physics* 1982; 21(3–4): 219–253. doi: 10.1007/bf01857727
26. DiVincenzo DP, Aliferis P. Effective fault-tolerant quantum computation with slow measurements. *Physical Review Letters* 2007; 98(2). doi: 10.1103/physrevlett.98.020501
27. Stoneham AM, Harker AH, Morley GW. Could one make a diamond-based quantum computer? *Journal of Physics: Condensed Matter* 2009; 21(36): 364222. doi: 10.1088/0953-8984/21/36/364222
28. Kreger-Stickles L, Oskin M. Microcoded architectures for ion-tap quantum computers. *ACM SIGARCH Computer Architecture News* 2008; 36(3): 165–176. doi: 10.1145/1394608.1382136
29. Solenov D, Brieler J, Scherrer JF. The potential of quantum computing and machine learning to advance clinical research and change the practice of medicine. *Missouri Medicine* 2018; 115(5): 463.
30. Flöther FF. The state of quantum computing applications in health and medicine. *Research Directions: Quantum Technologies* 2023; e10: 1–10. doi: 10.1017/qut.2023.4
31. Landman J, Mathur N, Li YY, et al. Quantum methods for neural networks and application to medical image classification. *Quantum* 2022; 6: 881. doi: 10.22331/q-2022-12-22-881
32. Jun K. A highly accurate quantum optimization algorithm for CT image reconstruction based on sinogram patterns. *Scientific Reports* 2023; 13(1). doi: 10.1038/s41598-023-41700-6
33. Wegner KD, Hildebrandt N. Quantum dots: Bright and versatile in vitro and in vivo fluorescence imaging biosensors. *Chemical Society Reviews* 2015; 44(14): 4792–4834. doi: 10.1039/c4cs00532e
34. Dixon T. The grey zone of cyber-biological security. *International Affairs* 2021; 97(3): 685–702. doi: 10.1093/ia/iiab041
35. Wierzbiński M, Falcó-Roget J, Crimi A. Community detection in brain connectomes with hybrid quantum computing. *Scientific Reports* 2023; 13(1). doi: 10.1038/s41598-023-30579-y
36. Marchetti L, Nifosì R, Martelli PL, et al. Quantum computing algorithms: Getting closer to critical problems in computational biology. *Briefings in Bioinformatics* 2022; 23(6). doi: 10.1093/bib/bbac437
37. Outeiral C, Strahm M, Shi J, et al. The prospects of quantum computing in computational molecular biology. *WIREs Computational Molecular Science* 2020; 11(1). doi: 10.1002/wcms.1481
38. Kamel Boulos MN, Zhang P. Digital twins: From personalised medicine to precision public health. *Journal of Personalized Medicine* 2021; 11(8): 745. doi: 10.3390/jpm11080745
39. Hashizume M. Perspective for future medicine: Multidisciplinary computational anatomy-based medicine with artificial intelligence. *Cyborg and Bionic Systems* 2021; 2021. doi: 10.34133/2021/9160478

40. Wahl B, Cossy-Gantner A, Germann S, et al. Artificial intelligence (AI) and global health: How can AI contribute to health in resource-poor settings? *BMJ Global Health* 2018; 3(4): e000798. doi: 10.1136/bmjgh-2018-000798
41. Ye Z, Yang J, Zhong N, et al. Tackling environmental challenges in pollution controls using artificial intelligence: A review. *Science of The Total Environment* 2020; 699: 134279. doi: 10.1016/j.scitotenv.2019.134279
42. Freedman MH. P/NP, and the quantum field computer. *Proceedings of the National Academy of Sciences* 1998; 95(1): 98–101. doi: 10.1073/pnas.95.1.98
43. Miyadera T. Quantum Kolmogorov complexity and information-disturbance theorem. *Entropy* 2011; 13(4): 778–789. doi: 10.3390/e13040778
44. Bernstein DJ, Lange T. Post-quantum cryptography. *Nature* 2017; 549(7671): 188–194. doi: 10.1038/nature23461
45. Malina L, Dzurenda P, Ricci S, et al. Post-quantum era privacy protection for intelligent infrastructures. *IEEE Access* 2021; 9: 36038–36077. doi: 10.1109/access.2021.3062201