UDC 004.932

DOI: 10.15587/1729-4061.2024.306968

DEVELOPMENT OF QUANTUM COMPUTING ALGORITHM OF TECHNOLOGY FOR MONITORING LEARNING RESULTS

Galiya Yesmagambetova
Corresponding author
Master of Technical Sciences*
E-mail: Gal.esm@mail.ru

Alimbubi Aktayeva
PhD**

Akky Kubigenova
Master of Technical Sciences*

Aigerim Ismukanova
Master of Technical Sciences*

Tatyana Fomichyova
Master of Technical Sciences*

Seilkhan Zhartanov
Master of Technical Sciences**

Aidyn Daurenova
Master of Technical Sciences**

*Department of Information and Communication Technologies
Kokshetau University named after Sh. Ualikhanov
Abay str., 76, Kokshetau, Republic of Kazakhstan, 020000

**Department of Information Systems and Informatics
Abay Myrzakhmetov Kokshetau University
Auezov str., 189 A, Kokshetau, Republic of Kazakhstan, 020000

The present publication considers implementing an online control proctoring system, with the possibility of using methods and models of pattern recognition using algorithmic quantum computing to conduct online exams. The study's object is the protection method within infrastructure proctoring systems in education. The study aims to create a security system for proctoring technology infrastructure in education. The article proposes an alternative approach to building protection systems with an effective recognition model using algorithmic quantum computing in proctoring platforms. This study addresses these issues and proposes a novel approach to generating a random cryptographic key using multimodal biometric technology. A presented quantum algorithm method for computer simulation of the data processing quantum principles allows studying and analysing how the created model for transforming a classical image into a quantum state works. This method also shows the possibilities of quantum information theory in interpreting classical problems or how to optimise the same, taking into account the development of methods for the functioning of models and algorithms for quantum computing, data protection and security of online video communications in a proctoring system in an educational environment. The novelty of this research is expressed primarily in the constant updating and addition of authentication systems using quantum computing in various aspects, including the proctoring system in the educational environment. The practical significance is due to the need in the current situation to attract attention to existing problems in structuring the infrastructure of a monitoring system within planning and coordinating the protection, thereby enhancing learning outcomes by eliminating security flaws using a quantum computing algorithm for pattern recognition

Keywords: quantum algorithm, qubit, entanglement, facial recognition technology, proctoring, educational environment

Received date 10.04.2024
Accepted date 13.06.2024
Published date 28.06.2024

***How to Cite** Yesmagambetova, G., Aktayeva, A., Kubigenova, A., Ismukanova, A., Fomichyova, T., Zhartanov, S., Daurenova, A. (2024). Development of quantum computing algorithm of technology for monitoring learning results. Eastern-European Journal of Enterprise Technologies, 3 (2 (129)), 69–82. https://doi.org/10.15587/1729-4061.2024.306968:*

1. Introduction

Modern education is also founded on implementing modern information and communication technologies, allowing two-way interaction. Innovative education has included networks of computers, communications, and digital satellites, as well as computer multimedia technologies and mixed educational technologies of different generations, such as information technologies, to achieve human-computer and interpersonal communication and interaction.

The increase in popularity and the extent of diverse e-learning resources and various forms of education are steadily rising. It has become crucial to possess the ability to effectively supervise online assessments for the advancement of the subsequent phase of academic instruction. Key components of the education system are teaching and proctoring examinations.

Professional proctors have been hired to monitor the entire examination process and ensure that exams are fair and that cheating has been detected. Interest in automated exam monitoring and mechanisms is growing. With confidence in the authenticity of a student's identity, the pursuit of a meaningful education is allowed, and the assessment of the knowledge and skills acquired by the student becomes reliable. Continuous validation (certification) should be conducted to maintain the accreditation's credibility. Validation should not be intrusive, disruptive, or distracting from the learning process at the same time.

Traditional proctoring has emerged as the predominant assessment method, necessitating students or test-takers to attend a designated examination venue or undergo test monitoring via a webcam. However, these methodologies are both costly and challenging [1].

One such technology is the automated proctoring system, which provides control over the conditions of the realization of control and evaluation activities of knowledge assessment and honesty of students, as well as support for the procedures of identification of the identity of learners. Proctoring technology, which involves visual observation of examinees during exams, is an integral part of educational assessment, and the ability to conduct visually proctored exams in real-time is a critical component of educational scalability. In the proctoring process, it's essential to monitor what's happening from a distance and confirm that the examinee is the one who needs to take the exam.

Educational institutions are eager to acquire cutting-edge technology to monitor cheating in exam rooms and ensure a cheating-free environment. For example, the proctoring system that utilizes a deep learning system achieved high accuracy for face detection and recognition, providing flexibility and accessibility for online classes while addressing the challenge of preventing cheating during exams [1].

The Online Examination Proctoring System aims to enhance the security and flexibility of online tests by incorporating user authentication, text detection, audio detection, and tab-switching detection components [2].

Proctoring technology, which involves visual observation of examinees during exams, is an integral part of educational assessment. The ability to conduct visually proctored exams in real-time is a critical component of educational scalability. Multifactor authentication and virtual reality technology have suggested improvements to create realistic exam environments and ensure only authorized users [2].

In the real-time proctoring process, it's essential to monitor what's happening from a distance and confirm that the examinee is the one who needs to take the exam. In real-time, action recognition by students or test-takers is challenging due to the inherently noisy nature of the interpretation produced by sensors, which are often subject to viewpoint occlusion, zoom, lighting, background clutter, camera movement, variations, and brightness.

When conducting online exam proctoring in environments with reliable infrastructure, it is also important to collect both quantitative and qualitative data, such as device details like processor type, clock speed, and RAM capacity, to better understand the challenges faced by exam candidates and improve future online proctoring technology solutions [3].

However, implementing online exam proctoring in different environments presents challenges, including high costs that not all educational institutions can afford, security concerns, privacy issues, and ethical considerations [2, 3].

Furthermore, limitations like unreliable infrastructure in low-resource settings, such as slow internet connections and a lack of compatible equipment, pose challenges to swiftly and efficiently proctoring online exams, emphasizing the need to carefully examine security constraints to deploy proctoring systems [4, 5].

Despite their labor-intensive and costly nature, let's propose a new framework to secure video sequences from educational activities. Faster encoding and decoding of images enable the application of quantum cryptography to streaming video, improving the security of online video communications, for instance, by utilizing a proctoring system in a learning environment.

The development of quantum computing is not just a technological advancement, it's a paradigm shift. It directly depends on the state of the art of the so-called 'hardware' for quantum computers. Projects for the development of quantum software, including cloud platforms for accessing quantum computers, have raised more than 100 million USD in total over the past two years. Quantum computers are not just capable of solving problems that are beyond the power of regular machines, they represent a promising method for a jump in computing performance. The present level of technology development may make the widespread introduction of quantum computing infeasible, but it's a field that has long been considered one of the most promising areas. The use of quantum algorithms with the advent of quantum computers exponentially increases the speed of solving computational problems, making our research in this area all the more significant and urgent.

The development of quantum computing and cybernate-associated technology in contemporary encryption implementations is only a matter of time. Given the potential cybersecurity threat, developing ways to protect against possible attacks is already the case. Nowadays, quantum pattern recognition algorithms spark great interest due to the emergence of the first quantum computers and software interfaces, focusing solely on the development and research of this area of computer science. Such an essential advantage of quantum algorithms in solving several complex computational problems and the lack of knowledge of their capabilities lead to the inference that research in this area is critical.

The topic being discussed is not just relevant, it's a pressing need in the current educational environment. The lack of practical and theoretical development of models for the architecture of modern proctoring systems is a gap that needs to be filled. The high speed of image encoding and decoding, made possible by quantum computing, will allow the use of quantum computing algorithms for streaming video. This will significantly increase the security of the proctoring system, making our research in this area a practical and necessary step forward.

Therefore, the studies of data privacy protection in image recognition in monitoring the educational process are relevant due to the need for more practical and theoretical development of data protection models and the security of online video communication for the infrastructure of modern proctoring systems in the educational environment.

2. Literature review and problem statement

The study [6] evaluates software engineering systematic review process research from 2005 to mid-2012, highlighting critiques, recommendations, and challenges. It emphasizes the need for continuous improvement and validation of tools and methodologies in this domain. The paper addresses vital criticisms, offers practical recommendations for process enhancement, and identifies challenges for more effective systematic reviews. It also highlights the persistent challenge of assessing the quality of studies using diverse empirical methods. However, the study's limitations highlight the need to acknowledge challenges and constraints to fully understand the scope and implications of the research. The study excluded papers mentioning process issues as an additional issue in a systematic review or mapping study to limit primary studies and reduce the number of documents needed to read, but this may not have included some relevant papers. The disadvantage of this study is that it is only a systematic review of research into software development processes and does not address data protection issues [6].

The paper [7] examines the legal issues arising from online proctoring technologies, focusing on data protection, human rights, and equality. It concludes that these technologies breach student rights and break the trust needed for learning. The over-reliance on exams as an assessment method is based on more innovative, inclusive, and rights-compliant methods. Proctoring technologies contradict basic principles of law and human rights legislation, as they assume exam-takers are bound to cheat. It also suggests that these technologies hinder the development of alternative assessment methods that promote inclusive learning. The disadvantage of this article is that it only considers the problems of using proctoring technologies in higher education and their possible legal consequences, including violations of data protection laws. It argues that the legality of the processing is controversial because assessment methods may violate students' rights. In addition, this work does not discuss strategies for protecting proctoring technology from hacking [7].

This paper [8] provides a thorough evaluation of various tools and offers practical recommendations for educational institutions where online proctoring faces challenges. These challenges include the need for access to suitable technological infrastructure, the digital divide between students, and the unique needs of students with disabilities. The paper also addresses concerns about the interpretation and use of recorded video. Students with disabilities may require specific assistance and tools. The disadvantage is that it is not about the design procedure methods protection of confidential data students that leads to providing purely subjective recommendations for implementing online proctoring that are comprehensive, including preparing university-wide recommended exam procedures, testing the system in actual courses with large numbers of students, providing a computer lab for students without laptops, and meeting hardware and software requirements for the system proctoring.

Within the paper [9], the study's key findings on proctored and non-proctored methods provide a comprehensive understanding of the effectiveness of proctoring technologies. The significant implication is that proctored systems resulted in lower test scores, regardless of grade or gender. The study suggests that while proctoring systems can prevent dishonest behavior among students, further improvements are needed, underscoring the potential of these technologies. The call for implementing supervised systems to eliminate unethical behavior among students is a clear path forward. The study's conclusion that the purpose of higher education is to instill values in students underscores the ethical considerations of proctoring technologies. The primary result of this research is that students exhibit positive attitudes towards using online proctoring. A key reassurance for educators is that integrating proctoring technology into Moodle is a straightforward process that requires no additional infrastructure. The disadvantage of incorporating such an approach is that with a data protection module, the system's online proctoring can be protected from hacking and attacks both inside and external [9].

Proposals posited in paper [10] suggest that the policy responses to address fairness, disparate test scores, and student testing in online classes. Online education is growing, but it also poses challenges, such as the perception that undetected cheating compromises academic integrity. Video proctoring significantly negatively affects online test scores because it discourages cheating. The study shows that proctoring software is essential to ensuring academic integrity by ensuring equal test-taking conditions in similar courses. This article also discusses that future research may influence the choice of proctoring, but the results highlight the need for proctoring software that will promote the integrity of online testing. The disadvantage is that the focus is on proctoring software, which is essential to ensuring academic integrity, rather than the design process of constructing an information security system for a proctoring system in education [10].

A paper [11] argues that, due to increased pressure to maintain high academic performance for future study or professional opportunities, students may experience test anxiety at some point in their higher education journey. Empirical observational studies have been conducted for decades to determine the psychological and physiological effects of test anxiety. This study examines the on-the-spot behavior exhibited by students while taking exams in an online course using a virtual proctor and how it relates to students' self-reported signs of test anxiety. Although a change in gaze direction may indicate academic dishonesty, educators must conduct a full investigation before concluding. The disadvantage is that the focus is on recommendations ranging from the need for targeted use of virtual proctoring to ensuring standards of academic integrity are offered, but this can be best achieved if instructor-proctors followed behavioural cues consistent with evidence of cheating [11].

In this article [12], the effects of proctoring on students' self-reported temptation to cheat and potentially undesirable side effects, including test anxiety, perceived exam difficulty, and performance, have been identified. This study showed that it is essential to consider a wide range of factors when deciding to implement proctoring, which are not solely related to reducing academic dishonesty. The disadvantage is that the focus is on time management, environmental structuring, learning strategies, and internet literacy, which could reduce test anxiety. The major disadvantage is that it is not a procedure for designing security systems against potentially unwanted side effects, including protecting students' self-reported temptation to cheat during testing.

This study's disadvantage [13] is that it only provides information on digital proctoring, an essential tool for improving academic integrity in online examinations and promoting digitalization in higher education. It guides practitioners in implementing digital proctoring systems and assesses their impact on students and teachers, but it needs to address the methods and models of data protection used because of proctoring technology.

In the paper [14], it is explicitly mentioned that the proctoring system exercises comprehensive control over the user's camera, microphone, and screen throughout the examination process, utilizing advanced technologies such as artificial intelligence, computer vision, and various other modules. Furthermore, this system furnishes the proctor with a detailed report that offers a segmented user behavior analysis. The document also asserts that the implementation of such exams leads to a reduction in organizational expenditures and an improvement in qualifications. However, the authors express uncertainty regarding the prolonged utilization of online proctoring technologies, raising questions about their efficacy and implications for the future.

In paper [15], posits the argument that biometric technologies play a pivotal role in identification and authentication, encompassing groundbreaking advancements that enable the assessment of students' physical and behavioral attributes. Biometric technologies have been used in identity management, class attendance, e-assessment, security, student motivation, and learning analytics. Using biometric data has advocated for executing academic and non-academic tasks within university settings. New features are being developed for commercial applications, such as vascular pattern recognition, ear shape recognition, facial thermography, odour detection, gait recognition, heartbeat authentication, brain waves, and human body bioacoustics. The disadvantage of this study is that it only provides researchers with a clear understanding of the potential of biometric technologies in education. It does not address students' issues with such systems because of privacy issues. However, security and privacy issues remain a significant concern.

Nonetheless, its utilization of proctoring technologies remains crucial to upholding academic integrity in online testing scenarios. All the papers we reviewed noted that proctoring plays a critical role in ensuring the integrity of online exams. It uses various technologies and methodologies to prevent academic dishonesty and allow for continuous monitoring. These systems provide real-time monitoring of exam processes, alerting teachers to any anomalies and providing a secure exam environment without physical testing equipment. However, the biometric technologies used in proctoring ensure only academic honesty. However, data protection problems, such as the protection of students' data, are not considered, and students' sensitive data needs to be protected. The comprehensive literature review has yielded invaluable insights and comprehension concerning integrating proctoring technologies within higher education institutions, encompassing discussions on technological advancements. There are also problems and peculiarities of authentication challenges and preserving students' confidential information. The findings underscore the urgency of developing more sophisticated proctoring software integrated with robust authentication protocols to bolster the integrity of online assessments.

3. The aim and objectives of the study

This study aims to develop an algorithm based on quantum computing, considering the features of the information security system of the proctoring infrastructure in education. This will allow will provide an objective assessment of the infrastructure and enhance the systems for protecting students' confidential data. This approach opens up new possibilities and underscores the urgency of developing protective measures for the security of the proctoring infrastructure.

To achieve this aim, the following objectives are accomplished:

– to evaluate and analyze approaches to pattern recognition using quantum computing algorithms;

– to compare the differences between traditional and quantum cryptography;

– to describe the classifications and a brief analysis of the characteristics of classical algorithms used in recognition;

– to develop an algorithm model for quantum cryptography facial recognition technologies.

4. Materials and Methods

The focus of the research is on the process of constructing an information security system for a proctoring system in the field of education. The current situation is not least due to the imperfection of the mechanisms used today to ensure the security of critical educational infrastructure facilities, including proctoring technology. The hypothesis of the research was as follows:

The proposal of a quantum cryptography algorithm-based face recognition model for security services in the proctoring system holds the potential to revolutionize the field of education, enhancing the security of critical educational infrastructure facilities.

The use of a quantum cryptography algorithm not only ensures high cryptographic strength and ease of implementation but also allows for the parallelization of image encoding and decoding processes, eliminating the need for complex computer technology. This practical approach also enables the transfer of various contents, including multimedia data.

In addition, research allows for the parallel processing of large data arrays of facial images using quantum correlations between the informative features of pictures. It implements an effective recognition method, enabling to build and ensure a confidential cryptosystem's required efficiency and reliability. In the future, it's planned to implement a proctoring system based on a university practically, and the main stages of the study of a security system have been formalized in the form of copyright [15, 16]. Thus, the proposed mechanisms allow for a methodological basis to construct a quantum cryptography algorithm for face recognition technologies proctoring systems.

5. Results of development of quantum computing algorithm

5. 1. Modern principles of pattern recognition and detection

The replenishment of the labor market with outstanding personnel is greatly facilitated and accelerated by modern Internet technologies in training and educating qualified specialists. Educational organizations have focused on constantly improving technologies oriented towards innovative growth models, which are necessary to rapidly implement modern technological innovations, especially those aimed at providing high-quality training, including distance learning. Proctoring increases the authenticity and reliability of the results by detecting the students' educational achievements. Most existing studies of proctoring systems have three detection modes: real-time proctoring, recorded proctoring and automated proctoring, but most are suitable for online exams only [15].

In line with the development of digital technologies in education, proctoring will be in demand more and more, and therefore, it is necessary to continue researching the possibilities of optimizing this process. However, to check the quality of training for students who master the profile remotely, it is essential to organize certification correctly.

The proctoring system, a comprehensive tool, plays a crucial role in online education. It verifies the identity of the participant, performs real-time surveillance to reveal possible violations, and conducts the identification of the person under an exam. The system observes its actions using a webcam and perceives what is happening on its computer monitor. This advanced technology allows, with a high degree of probability, to confirm the identity of the examinees, objectively assess their knowledge, and exclude cheat sheets and other tricks during the exam (Fig. 1).

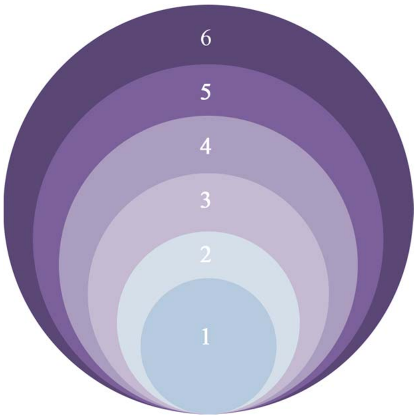


Fig. 1. Principles of Proctoring in the Education System: 1 — independence; 2 — objectivity; 3 — tonality; 4 — relevance; 5 — control; 6 — orderliness [10]

The proctoring technology provides a means of monitoring the conditions for the implementation of control and evaluation activities. It ensures organizational support for procedures for confirming the identity of students (Fig. 2).

A mixed proctoring system is often used, working as follows: a video recording of the exam with the comments of the program is additionally viewed by a person who decides whether violations indeed took place (Fig. 3).

Generally speaking, due to human supervision's limitations and the lack of effective proctoring systems, a new efficient proctoring system based on quantum computing and facial recognition technologies is needed to assist in offline examinations.

The limitations of classical cryptographic methods have paved the way for the innovative development of quantum cryptography. Unlike classical cryptography, which is based on mathematics and the computational difficulty of factorizing large numbers, quantum cryptography is an emerging technology that harnesses the unique phenomena of quantum physics. It enables two parties to have secure communication, leveraging the invariability of the laws of quantum mechanics. Fig. 4 provides a visual comparison of classical and quantum cryptography.

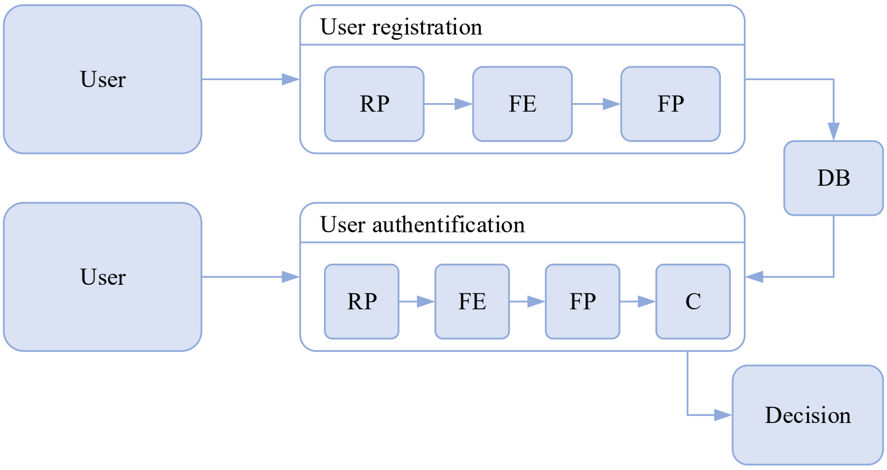


Fig. 2. General diagram of the functioning of the biometric user authentication system: RP — readout the biometric parameter of the user; FE — feature extraction from obtained biometric parameter; FP — feature processing and creation of a biometric template for a given user; DB — save the obtained template in the system database; C — Comparator [10]

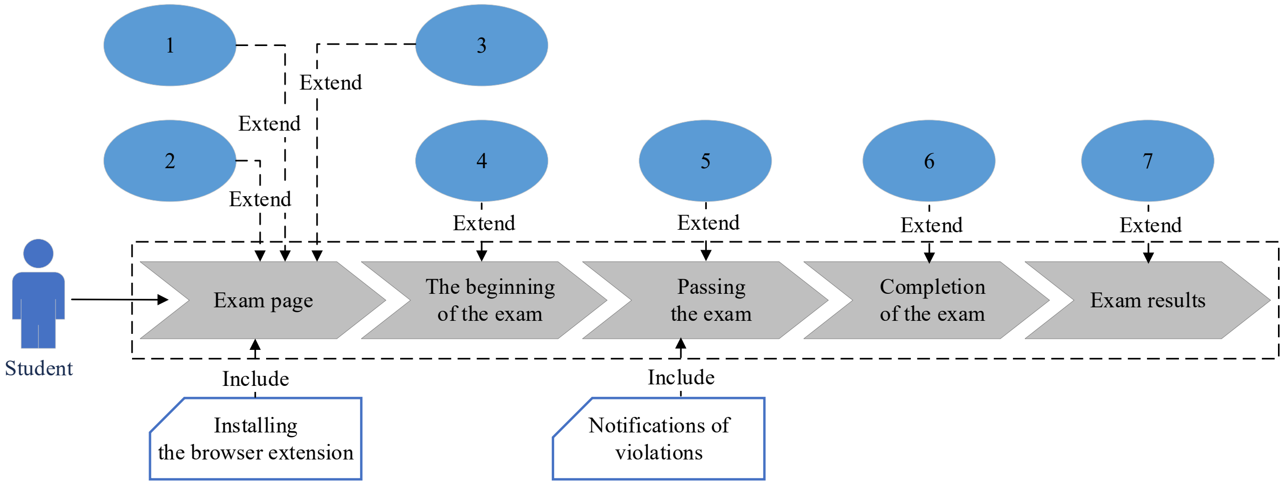
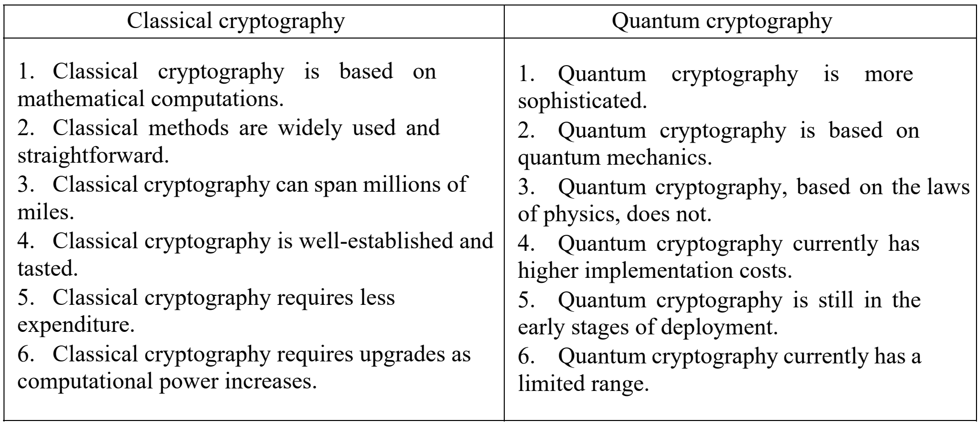


Fig. 3. Embedding proctoring functions in the script for passing the exam of the on-line learning system: 1 — exam registration (API: register.); 2 — authorization (API: authorize.); 3 — checking the connection (API: check.); 4 — starting surveillance (API: start.); 5 — tracking violations (API: deflect.); 6 — stopping surveillance (API: stop.); 7 — requesting result (API: fetch.) [10]



Classical cryptography	Quantum cryptography
1. Classical cryptography is based on mathematical computations. 2. Classical methods are widely used and straightforward. 3. Classical cryptography can span millions of miles. 4. Classical cryptography is well-established and tasted. 5. Classical cryptography requires less expenditure. 6. Classical cryptography requires upgrades as computational power increases.	1. Quantum cryptography is more sophisticated. 2. Quantum cryptography is based on quantum mechanics. 3. Quantum cryptography, based on the laws of physics, does not. 4. Quantum cryptography currently has higher implementation costs. 5. Quantum cryptography is still in the early stages of deployment. 6. Quantum cryptography currently has a limited range.

Fig. 4. Analyzing the differences between traditional and quantum cryptography

A quantum computer, a device capable of performing quantum computations, is a marvel of modern technology. It uses controlled manipulation of quantum states of qubits to execute algorithms. Unlike a traditional computer, a quantum computer can acquire an arbitrary quantum state from an arbitrary input quantum state. This unique ability allows quantum computers to precisely calculate the behavior of quantum systems or minuscule particles, as detected by quantum mechanics, opening up a world of possibilities.

Quantum computing is a rapidly evolving technology that could have far-reaching implications for industry and every sphere of modern life. Quantum computing is a powerful tool based on qubits, units of quantum information capable of possessing two states simultaneously: 0 and 1. Taking advantage of the principles of quantum mechanics, quantum computers can perform calculations much faster than conventional computers, which use transistors and logic gates to process information.

Quantum computing may reduce the time and resources required to develop products and processes, making creating or improving new products more accessible and faster. In addition, quantum computing helps optimize the business processes of educational organizations that require a large amount of computing in a much shorter time, leading to more efficient and cost-effective educational process management.

Facial recognition is a technology used to identify personalities or groups of people in stable images and videos. Facial recognition is a type of computer vision that uses optical input to analyze an image. In this case, all the faces in the image have been viewed. In more detail, the process of face recognition in images can be represented by the following steps:

1. Image preprocessing, which is necessary to put the image into a standard format convenient for recognition.

2. Selection or detection of faces in the image.

3. Extraction and encoding of the most representative features (characteristics) of faces from Fig. 11.

4. Comparing the faces in the image to those stored in the database to determine the reliability of recognition (Fig. 5).

The intricacy of the facial recognition process is evident in the various ways each stage can be implemented. Some algorithms can be used simultaneously in multiple stages, adding to the complexity. The efficiency of a facial recognition algorithm, a key measure of its success, is determined by the quality of recognition (as indicated by the percentage of correctly identified images relative to the percentage of false positive classifications). This, in turn, is influenced by the methods and algorithms available for image analysis and the speed of these algorithms, which is a product of the quality of the software implementation and the hardware used.

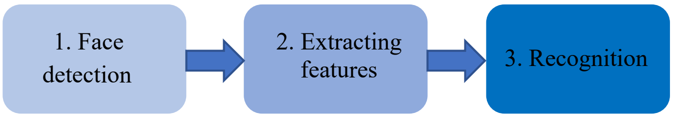


Fig. 5. General face recognition scheme

Problems arising in the process of face recognition may include variations in the set of face images, such as race, gender, emotions, lighting, and head position, as well as the presence of masking features (glasses, moustaches, closed eyes, etc.). As mentioned in [17], to model the problems of pattern recognition and detection on quantum computers, it is necessary to work on two areas:

– to develop methods for creating quantum algorithms that process images by converting classical image processing algorithms into quantum algorithms (equivalent to classical computer vision algorithms);

– to study the applicability of quantum neural networks in detection and recognition tasks.

One of the most crucial tasks in the facial recognition process is the selection of an appropriate similarity measure for two sets of descriptors corresponding to the features of face images. This decision significantly impacts the accuracy and reliability of the recognition system. Currently, similarity measures based on the cross-correlation of two images are widely used, underscoring the importance of this choice (Table 1).

Such a solution to the recognition problem is combinatorial and seeks further improvement. Quantum image recognition and processing algorithms can be considered a separate category.

Table 1

Main measures of image similarity based on cross–correlation [18]

No.	Measure of similarity	Formula
1	The sum of absolute differences, SAD	$\sum_{(i,j\in W)} \left|I_1(i,j)-I_2(x+i,j+j)\right|$
2	Zero-mean sum of absolute differences, ZSAD	$\sum_{(i,j\in W)} \left|I_1(i,j)-\overline{I}_1(i,j)-I_2(x+i,y+j)+\overline{I}_1(x+i,y+j)\right|$
3	Locally scaled sum of absolute differences, ZSAD	$\sum_{(i,j\in W)} \left|I_1(i,j)-\frac{\overline{I}_1(i,j)}{\overline{I}_2(x+i,y+j)}I_2(x+i,j+j)\right|$
4	The sum of squared differences, SSD	$\sum_{(i,j\in W)} \left(I_1(i,j)-I_2(x+i,j+j)\right)^2$
5	Zero-mean sum of squared differences, ZSSD	$\sum_{(i,j\in W)} \left(I_1(i,j)-\overline{I}_1(i,j)-I_2(x+i,j+j)+\overline{I}_2(x+i,y+j)\right)^2$
6	Locally scaled sum of squared differences, LSSD	$\sum_{(i,j\in W)} \left(I_1(i,j)-\frac{\overline{I}_1(i,j)}{\overline{I}_1(x+i,y+j)}I_2(x+i,j+j)\right)^2$
7	Normalized cross correlation, NCC	$\frac{\sum_{(i,j\in W)} I_1(i,j)I_2(x+i,j+j)}{\sqrt{\sum_{(i,j\in W)} I_1^2(i,j)-I_2^2(x+i,j+j)}}$
8	Zero-mean normalized cross correlation, NCC	$\frac{\sum_{(i,j\in W)}\left(I_1(i,j)-\overline{I}_1(i,j)\right)\left(I_2(x+i,j+j)-\overline{I}_2(x+i,j+j)\right)}{\sqrt{\sum_{(i,j\in W)}\left(\left(I_1(i,j)-\overline{I}_2(i,j)\right)^2\sum_{(i,j\in W)}\left(I_2(x+i,j+j)-\overline{I}_2(x+i,j+j)\right)\right)}}$
9	The sum of Hamming distances, SHD	$\sum_{(i,j\in W)} \left(I_1(i,j)\,\mathrm{XOR}\,I_2(x+i,j+j)\right)$

5. 2. The variations between conventional and quantum cryptography

Quantum computing is a new type of computing that is expected to change computer systems in the future fundamentally. Since quantum mechanics is a more general model of physics than classical mechanics, it leads to a more general model of computation capable of solving problems impracticable for classical computation. The principles of quantum mechanics are employed in quantum computing to process and manipulate information. In addition to the principles of quantum mechanics, quantum computing enables it to perform certain types of calculations much faster than classical computing [19].

Unlike classical computers, which use bits as the minor data units represented as 0 or 1, quantum computers use quantum bits or qubits, which can exist in a superposition of states, representing both 0 and 1 simultaneously. Four numbers are required to identify the state uniquely; a pair of two qubits can be in a superposition of four states. The possible states of 0 or 1 in qubits can make the photon polarization vertical or horizontal (Fig. 6).

Based on the quantum properties of "superposition and "entanglement" n qubits can act as a group or in isolation, resulting in an exponentially greater information density than a classical computer. In general, the quantity of data kept in N qubits corresponds to 2 raised to the power of N (2^N) conventional bits.

Quantum computing achieves polynomial speedup if it solves a problem in time T for which a classical computer requires time T^2 or some other polynomial function of T. Similarly, quantum computing achieves exponential speedup if it solves a problem in time T for which a classical computer takes time 2^T or another exponentially growing function of T.

A quantum bit is the fundamental unit of information used in quantum computers. This can be compared to a bit that is used in a classical computer. A qubit, in more technical terms, is a two-dimensional quantum system. The state of a qubit can be expressed as:

$$|\phi\rangle=\alpha|0\rangle+\beta|1\rangle, \qquad (1)$$

where α and β are complex numbers and $|\alpha|2+|\beta|2=1$. In ket-notation or Dirac notation, $|0\rangle=(10)$ and $|1\rangle=(01)$ are used to represent the basic states of a two-dimensional vector space. Therefore, equation (1) truly shows the state of the qubit as a two-dimensional complex vector ($\alpha\beta$).

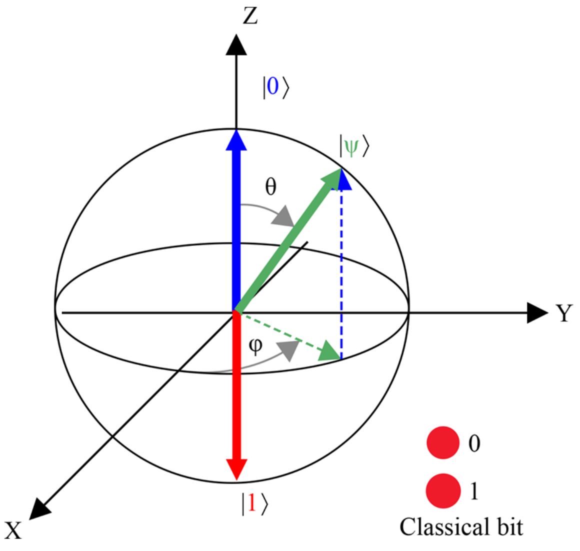


Fig. 6. Classic bit and Qubit [5]

The difference compared to a classical bit is that a qubit cannot be measured without changing it. Measuring a qubit or its state given by equation (1) will give a classical value equal to zero ($|0\rangle 0$) with probability $|\alpha|2|$ or one ($|1|1$) with a probability of $|\beta|2|$. In addition, $|\phi\rangle$ (the conjugate transposition of $|\phi\rangle$) is a row vector (known as bra) with two components: $\langle 0|=(10)$ and $\langle 1|=(01)$. From bra and ket, it is possible to compute the inner or outer products of the vectors. Given $|u\rangle$ and $|\upsilon\rangle$, their inner product is $\langle u|\upsilon\rangle(=\langle u||\upsilon\rangle)$, which is a scalar. For example, $\langle 0|0\rangle=\langle 1|1\rangle=1$ and $\langle 0|1\rangle=\langle 1|0\rangle=0$. The outer product is obtained using $\langle u||\upsilon\rangle$ and is an operator in matrix form. If $|0\rangle\langle 0|0\rangle\langle 0$ (i. e., $\langle 0|$ works on $|\phi\rangle$, the result is $\alpha|0\rangle$.

This means that the operator $0\rangle\langle 0|0\rangle\langle 0$ will extract the $|0\rangle 0$ component from $|\phi\rangle$ or $|\phi\rangle$ measured in the $0\rangle 0$ direction. Similarly, the operator $|1\rangle\langle 1$ extracts $|1\rangle\langle 1$ components from $|\phi\rangle$. The efficiency of quantum computing is determined by the number of reproducible qubits and the maintenance time of quantum superposition.

Quantum computing algorithms have been developed for combinatorial problems, optimization problems, and specific simulations. The model of quantum algorithms is based on the physical laws of the theory of quantum computing, namely that unitary, reversible quantum operators are involved in the calculations. To sum up, a quantum algorithm consists of three main unitary operations:

1.Superposition.

2.Quantum correlation (quantum oracle or entangled operators).

3.Interference [20].

The fourth operator, the operator for measuring the results of quantum computations, is irreversible (classical). The fundamental result of the theory of quantum computing states that all operations can be implemented on a scheme consisting of universal basis elements. Unlike their classical counterparts, quantum algorithmic cells (QAC) can be implemented on different classes of universal elements, depending on the computational basis used.

Quantum algorithmic cells with fixing computationally and measurement bases depict the evolution of some unitary operator U, to which the quantum computational process $|\psi_{\mathrm{fin}}\geq U||\psi_{\mathrm{in}}\rangle$ corresponds, where the vector (wave function) $|\psi_{\mathrm{in}}\rangle$ sets the initial conditions for the calculation (of the problem being solved), and $|\psi_{\mathrm{in}}\rangle$ fin reflects the result of the calculation due to the action of the operator U on the initial state $|\psi_{\mathrm{in}}$. Various forms of the operator U (in particular, the Hamiltonian) result in different models of quantum computing. In general terms, the quantum computing model consists of five stages:

– preparation of the initial (classical or quantum) state ψ_{in};

– performing the Hadamard transformation for the initial state to prepare the superposition state;

– application of an entangled operator or a quantum correlation operator (quantum oracle) to a superposition state;

– execution of the interference operator;

– use of the measurement operator for the result of quantum calculations $|\psi_{\mathrm{in}}\rangle$ [20, 21].

Quantum algorithms are often presented as quantum circuits consisting of quantum gates that process input qubits. Various combinations of quantum gates can execute a particular quantum algorithm, the results of which are obtained by quantum measurement. Quantum gates and operators are applied qubits. In the schematic diagram, the qubit is represented by a horizontal line. This is done clockwise from the left. The initial state of the qubit is shown on each line. Control is shown in the same order as it is applied from left to right. The state of a qubit in a quantum circuit changes with time [21].

Mathematically, a unitary matrix is used to represent a quantum gate, and the number of qubits at the input and output of the gate must be equal. Measuring elements are used to measure the qubits in the computational infrastructure. The measurement element is identified by a unique element with a metric symbol.

5. 3. Classifications and a brief analysis of the characteristics of classical algorithms used in recognition

In 1982, it was empirically demonstrated and validated through rigorous scientific inquiry that in the realm of quantum problem-solving, the intricacy and sophistication of arriving at a solution using traditional computing methodologies experience a substantial and remarkable surge in complexity, exhibiting an exponential growth pattern that is directly contingent upon the specific input variables involved in the computational process, indicating that the task at hand becomes exceedingly arduous and impracticable to accomplish through conventional means, thereby necessitating the utilization of advanced quantum computing technologies and techniques.

The main advantages of using quantum calculations in defining objects and images include acceleration of the computational process using quantum components, stability at different angles of the object, its movement and statics, and ensuring cryptographic noise immunity. A hybrid quantum-classical system usually consists of quantum and classical parts. The first step in the quantum part is a (fixed) state preparation scheme called an encoding scheme. The two most common encoding types are qubit encoding, which encodes data into individual qubits, and amplitude encoding, which encodes data into the amplitude of a tangled set of qubits [22].

The most crucial stage of the quantum part consists of a parametrized quantum circuit (also called PQC or QNN) with parameters corrected in the classical part. The output of the quantum part is the classical value obtained by the measurement.

The classical part applies an optimization algorithm to adjust the parameters of the quantum circuit. In addition, the classical part may also perform pre-processing and post-processing of the classical data. Thus, a hybrid quantum-classical system can utilize quantum computing and classical processing and optimization techniques [21, 22].

Facial recognition technologies on video surveillance records require the creation of methods for fast processing of large amounts of data and "smart" systems capable of comparing images and distinguishing them from each other. Contemporary developed quantum systems are suitable for these tasks because, unlike present-day computers, they will have a hundred-fold more processing power. Such technological solutions require new algorithms.

The possibilities of face recognition technologies in quantum computing are just beginning to be explored. Continued research might bring in more applications for this powerful technology. The capabilities of facial recognition technologies could revolutionize computing, and quantum computing could soon be used in a wide variety of applications [22].

Face recognition technology may be a building block to support other capabilities such as face identification, grouping, and verification. Facial recognition software provides many practical use cases for businesses and education (proctoring).

In the past, computer vision methods were used for pattern recognition and detection, i.e., technologies that could detect, track, and classify objects. In recent times, the tasks of pattern recognition and detection have been actively used by machine learning and artificial intelligence technologies, including such areas as Deep Learning and Neural Networks. A precise dynamic partial replacement method for computer vision algorithm libraries by deep artificial neural networks already exists, which cope well with classifying and identifying objects, phenomena, processes, and situations.

Artificial neural networks (ANNs) have proven their usefulness, so it is not surprising that quantum neural networks (QNNs) have been attracted to this area. Due to the quantum mechanical effects, these networks can perform computation faster than classical ANNs. One of the possible classifications of face recognition techniques is as follows.

Shape-based (uses information about the relative position and size of features). Requires thresholds to be set-examples: Harris detector, Harris-Laplace detector, SUSAN (Smallest Univalue Segment Assimilating Nucleus), etc.

Template-based. It is inconvenient because templates must design in advance, and it is complex to design robust templates.

Color-based segmentation. It is disadvantageous in that features can only be extracted from frontal or proximity images of faces.

Appearance-based approaches (ASM, AAM, PCA, ICA, Gabor wavelets, and resource-intensive approaches regarding memory usage and CPU time).

In addition, training and manual placement of contours and landmarks in the image are required; approaches such as PCA, ICA, and Gabor wavelets are more natural to use for face detection than feature extraction. Hybrid techniques assume that if the feature extraction and encoding tasks are adequately resolved, the recognition task is trivial and reduced to finding instances in the face database that minimizes the distance to the object to be classified. The shortcomings of modern image recognition techniques are as follows:

– errors when searching large databases;

– recognition errors when changing the angle of the object;

– effects of lighting on recognizing quality;

– ageing changes;

– signs of masking;

– software sensitivity to facial expressions [23].

The way users recognize faces is highly dependent on the level of illumination, angle, and quality of the photo recorder and is also sensitive to changes with ageing and facial expressions [23].

Personal identification systems based on analyzing a single biometric parameter (uni-modal) can be bypassed if a digital copy of a person's face or voice is created. The disadvantages of the procedure for recognizing a person from a face image include a strong dependence on the degree of illumination and the head's rotation angle. The quality of the optical device also affects the accuracy of this kind of biometric system. It is essential when monitoring crowded places, such as stadiums, subways, and airports, where the distance from the video camera to the object might comprise tens of meters. Also, facial recognition algorithms are sensitive to age-related changes. Over time, a person may change their hairstyle, a beard or moustache may appear, and glasses, which ultimately complicates the task of identification [23].

Fig. 7 presents the multi-modal biometric identification systems, which consist of a standardized technique that includes four building blocks: a data capture module, a feature generation module, a comparison module, and a decision module.

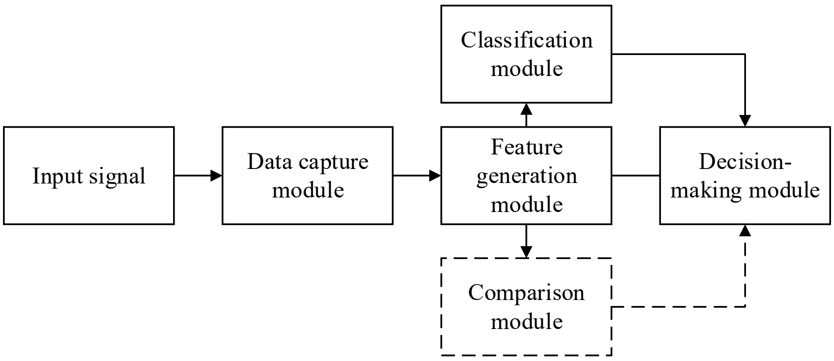


Fig. 7. Structural diagram of a multi-modal biometric identification system

The authentication algorithm may encounter a problem when user registration is performed in near-ideal conditions and testing and operation of the device occur in a high-noise environment. The inability to control external factors and non-compliance with the rules for collecting biometric data can significantly reduce the accuracy of such a system. As a consequence, it is necessary to develop more advanced personality identification algorithms. One of the promising directions in developing biometric systems is developing and researching personality identification algorithms based on two or more biometric parameters, the so-called multi-modal solutions based on quantum computing.

The approach based on the combination of modalities allows not only the increase of the stability and accuracy of biometric systems but also the improvement of their reliability in case of unauthorized access attempts. The need for such algorithms remains at its highest level. As a result, personality identification algorithms need to be developed, considering that people can work in real-world practical conditions.

5. 4. Algorithm model for quantum cryptography of facial recognition technologies

The main purpose of the proposed algorithm for converting a classical image into a quantum state is to convert the original image into a quantum form for the purpose of subsequent application of quantum algorithms (Fig. 8), for example, Grover's algorithm or quantum geometric transformations. The algorithm's operation involves applying a series of quantum operations to the input state, which is initially a superposition of all possible transformation states. Grover's algorithm relies on the idea that amplifying the amplitude of the marked state is achieved by applying a quantum operation iteratively [23].

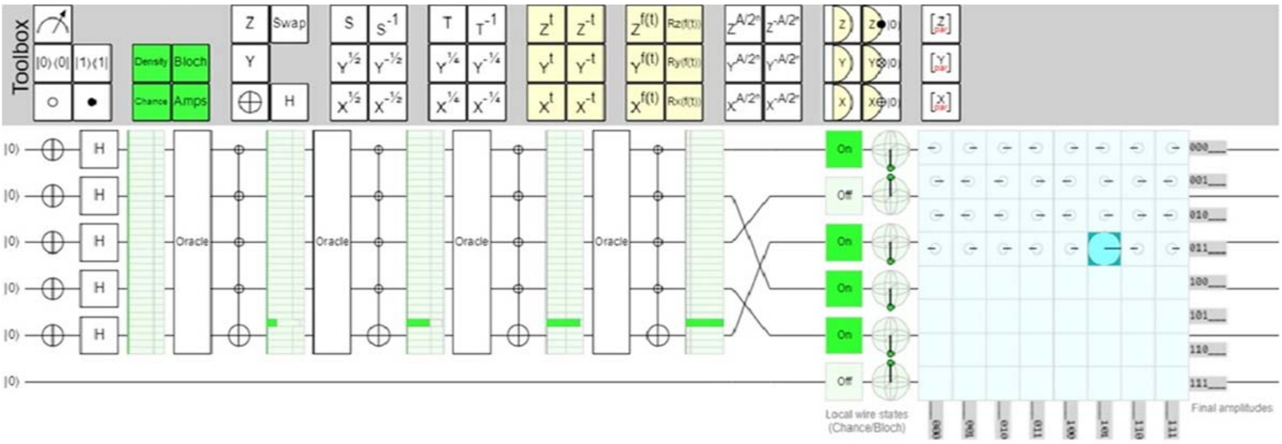


Fig.8. Diagram Grover's algorithm

This quantum approach to image representation and processing assumes that each image pixel $x(i, j)$ shall be transformed into a quantum state |q(i/j)⟩:

$$|q(i,j)\rangle = c_0|0\rangle + c_2|1\rangle, \tag{2}$$

where $|c_0|^2$ and $|c_0|^2$ mean a probability that after the measurement the state will be $|0\rangle$ or $|1\rangle$, respectively, and the following condition is satisfied: $|c_0|^2$ and $|c_0|^2=1$.

It should be noted that the choice of the initial values of the probability amplitudes that encode the colors of the image pixels can be different and depend on the algorithm used to convert the image into a quantum form. In addition, depending on further transformations, it may be necessary to create a superposition of pixels in the input image. The superposition is created by several steps:

1. Coding of pixel colors (represented as real numbers) into complex amplitudes of quantum states:

$$\delta: R^3 \to C_1^2(x_1,x_2,x_3) \to \left(r_1e^{i\phi_1}, r_2e^{i\phi_2}\right), \tag{3}$$

where x_1, x_2 and x_3 are the components of the RGB color model (red, green, blue);

$$r_1 := \sqrt{1-x_3^2},\quad r_2 = x_3,$$

$$\phi_1 := \arcsin(2x_1-1),\quad \phi_2 := \arcsin(2x_2-1).$$

2. Suppose:

$$z_1 = r_1e^{i\phi_1},\quad z_2 = r_2e^{i\phi_2},\quad \mathrm{z}_1 = \mathrm{r}_1\mathrm{e}^{\mathrm{i}\phi_1},\quad \mathrm{z}_2 = \mathrm{r}_2\mathrm{e}^{\mathrm{i}\phi_2}.$$

The pixel color shall be: $|q_i\rangle = z_0|0\rangle + z_2|1\rangle$.

3. The reverse transformation is performed as follows:

$$\gamma: C_1^2 \to R^3,\quad (z_1,z_2) \to \left(\frac{1+\sin\phi_1}{2}, \frac{1+\sin\phi_2}{2}, |z_2|\right), \tag{4}$$

where $\phi_1 := \arg(z_1)$, $\phi_2 := \arg(z_2)$.

4. Pixel coordinates are encoded as follows:

$$|k = |x|y = |x_{n-1}x_{n-2}\ldots x_0|y_{n-1}y_{n-2}\ldots y_0, x_i,\quad x_i \in \{0,1\}, \tag{5}$$

where the states $|x$ and $|y$ encode pixel coordinates (column and row numbers of a pixel, respectively).

As a result, let's obtain a superposition of the quantum states of the pixels of the input image in the form:

$$|I\rangle = \frac{1}{2^n}\sum_{k=0}^{2^{2n}-1}|q_k\rangle \otimes |k\rangle. \tag{6}$$

As a consequence, the transformation technique depicts a multi-pixel image as a single superposition including the properties of all pixels in the image. In the quantum computing model, the probability amplitudes and the state vector are members of a superposition and must be stored as separate values, while the pixels are stored in a conventional computer. The quantum cryptography algorithm of facial recognition technologies is an extension of the classical cryptography algorithm and is designed to encode images in the course of exchanging secret information. Restoring the original image from a quantum superposition is more complicated.

Consider the results of decoding a classical image from a quantum superposition state – a quantum visual secret exchange scheme. Having an image of size $M\times N$, from which it is required to get two "shadow" images of size $2M\times 2N$ each. Let's transform each pixel of the input image $x\ (i, j)$ into a quantum state $|q$ (i, j), which is a superposition of four basic quantum states the |00, |01, |10⟩and |11⟩, i. e.:

$$|q\ (i,j)\rangle = c1|00\rangle + c2|\ 01\rangle + c3|\ 10\rangle + c4|11\rangle.$$

The probabilities of measuring each base state are equal, i. e.:

$$|c1|2 = |c1|2 = |c3|2 = |c4|2 = 1/4.$$

For each basic state of the |00⟩, |01⟩, |10⟩ and |11⟩, a one-to-one correspondence is selected from the set of possible states of a group of pixels that characterize each pixel of the original image in the "shadow" image.

For instance, a group of pixels $\begin{bmatrix}1 & 0\\ 1 & 0\end{bmatrix}$ might correspond to the |00⟩states, the group $\begin{bmatrix}0 & 1\\ 0 & 1\end{bmatrix}$ might correspond to |01 states, the group $\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$ corresponds to |10, and the group $\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$ to the state |11.

According to the basic quantum state let's obtain by measuring the quantum state of a pixel in the original quantum image, the corresponding color will be chosen for the pixel, representing one of the classical "shadow" images of the pixel in the original image. The technology for facial recognition systems based on intelligent quantum computing will allow parallel processing of large data arrays of face images and, using the quantum correlation between informative features of images, implement an effective recognition method.

The task of concealing visual information is the reverse of the task of recognition. The technology developed for facial recognition systems in images and videos is based on the use of intelligent facial recognition quantum computing technologies. Additionally, the obtained quantum cryptography diagram of facial recognition technologies inherits most of the advantages of the classical scheme and also expands its capabilities (Fig. 9).

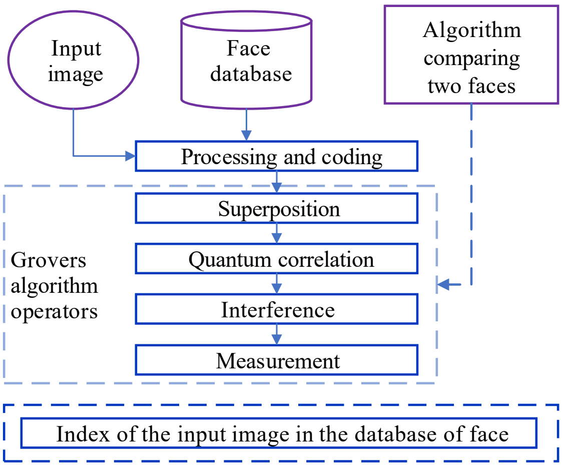

Input image
Face database
Algorithm comparing two faces
Processing and coding
Superposition
Grovers algorithm operators
Quantum correlation
Interference
Measurement
Index of the input image in the database of face

Fig. 9. Diagram of quantum face recognition [23]

By combining the foundations of quantum algorithms with available classical algorithms, it is possible to implement an effective face recognition system that solves (in whole or in part) many of the above shortcomings. Advantages of Using Hybrid Computational Algorithms for Face Recognition:

– potential for faster computation through the use of quantum evolutionary operators;

– the introduction of quantum operators of superposition and correlation to classical algorithms, as well as the stochastic nature of quantum algorithms, involves the emergence of the unique properties of the data processing process that affect the outcome of the algorithm;

– radically new approaches to the description of face recognition algorithms and cryptography and stenography algorithms;

– immaterial dependence on environmental interference;

– no dependence on stationary or moving objects or cameras;

– transmission of a full-fledged video image over low-speed communication channels;

– ensuring a high level of security when trying to interfere with image control channels [24–26].

The algorithmic model of quantum cryptography for face recognition techniques can be used independently or in conjunction with other quantum cryptographic algorithms for image and video processing.

6. Discussion of the results of adapting proctoring technology in education on the integration of quantum computing algorithms with biometrics data

The development of proctoring systems demands new approaches to building security systems. At the same time, experts question the possibility of using classical cryptographic cryptosystems to provide a modern security level. A new approach that considers the characteristics of educational platforms and security systems is essential in building systems. It's crucial to contemplate the possibility of categorizing information resources based on the technologies employed in proctoring.

In this study, an advanced requirement to develop a protection system for proctoring has been devised for a face recognition model that utilizes a quantum cryptography algorithm.

A feature of the proposed solution is that such quantum algorithms allow the construction of stable cryptosystems, such as those that provide the necessary level of efficiency and reliability during complex proctoring in the educational environment.

Quantum algorithms have demonstrated that security services can be provided through a combination of cryptographic mechanisms and robust coding methods using multimodal biometric technology [27].

The standards continue to consider security components and outline the threats and preventive action mechanisms for every data protection component [28]. Implementing this algorithm has significant implications that go beyond improving protection experiences and have the potential to transform the proctoring system in educational institutions completely. This approach needs to allow an objective assessment of the current state of the protection system and the possibility of proctoring due to the hybrid nature of threats or their integration with social engineering methods.

The research outcomes regarding the classic authentication scheme in the proctoring technology were critiqued for its vulnerability if an attacker acquires logins and passwords. To address this, the proposed solution introduces an authentication process employing multimodal biometric technology with quantum algorithms for protection.

To ensure further development of quantum algorithms with multimodal designs of biometric technology, it's proposed that stable-level system protections be modified. This approach provides the necessary level of system protection without compromising security. An advantage of the model is that, through various modifications in the choice of solutions, this approach to data will not only reduce computer and financial costs but also improve security.

The proposed mechanism will maintain the required security level, which will prevent proctoring systems from being hacked. Fig. 2 presents a methodology for constructing the functioning of biometric user authentication systems, providing an objective assessment of the current state of security of the infrastructure of proctoring technologies in the educational environment.

Quantum algorithms will be the foundation of a security system that provides:

– the necessary level of security;

– taking into account the secrecy of information resources;

– their circulation;

– and their storage.

Fig. 9 depicts the obtained quantum cryptography diagram for facial recognition technology, which retains most of the benefits of the classical scheme while significantly expanding its capabilities.

The proposed quantum algorithms offer protection through multimodal biometric authentication and encrypted storage of access links in the proctoring system that provide the necessary level of security and emphasize the need for robust security in personal data for students.

The biometrics-based authentication model presents a standardized module that includes preprocessing (1), feature extraction (2), feature comparison (3), and (4) authentication processes [29, 30]. The proposed approach is to replace the fourth modulus of authentication with quantum algorithms that use unique multimodal biometric features. The model then increases the authentication model's dependability by establishing a systematic and secure technique for authenticating based on unique multimodal biometric features utilizing quantum computing.

The limitation of the study is due to factors such as security and privacy when implementing electronic monitoring in educational institutions. However, this limitation should be addressed in future research and extended to other security-relevant factors affecting this implementation by studying the protection module weaknesses of various technology tools.

In the future, let's add modules relevant to implementing various methods directly onto the proctoring platforms, which will help provide a good starting point for an enjoyable experience with visual learning tools. This can only be accomplished by thoroughly analyzing the request and swiftly deciding on a quantum computing simulation method. Accordingly, testing the model will be possible with various approaches to pattern recognition and detection in the proctoring system for better problem-solving and performance analysis.

In conclusion, this study provides a foundation for future research on applying algorithm models for quantum cryptography in facial recognition technologies, presenting new avenues for enhancing the accuracy and efficiency of the transformation of technology for monitoring learning results. In the future, a promising direction is the use of artificially intelligent neural networks, which will expand the range of analysis of threats and vulnerabilities by providing the necessary level of objectivity for taking preventive measures.

7. Conclusions

1. Analysis and evaluation approaches show that quantum computing uses controlled manipulation of qubit states to perform algorithms, reducing time and resources for development and improving existing ones. It can optimize business processes in educational organizations, leading to more efficient management. Facial recognition is a technology that identifies personalities or groups in images and videos. It depends on the quality and speed of the recognition algorithms. To model pattern recognition and detection on quantum computers, researchers need to develop methods for creating quantum algorithms and study the applicability of quantum neural networks in detection and recognition tasks.

2. Due to preliminary calculations, a procedure for quantum algorithmic cells represents the evolution of a unitary operator U, which corresponds to the quantum computational process. The model of quantum computing consists of five stages: preparation of the initial state, Hadamard transformation, application of an entangled operator or quantum correlation operator, execution of the interference operator, and use of the measurement operator for quantum calculations. Quantum gates and operators process input qubits, with the qubit's state changing with time. A unitary matrix represents a quantum gate and measuring elements used to measure qubits in the computational infrastructure.

3.Describe the classifications and briefly analyze the characteristics of classical algorithms. They show that face detection in image recognition requires training and manual placement of contours and landmarks, with approaches like PCA, ICA, and Gabor wavelets being more natural. Also, hybrid techniques assume that if feature extraction and encoding tasks are adequately resolved, the recognition task is trivial and reduced to finding instances in the face database that minimizes the distance to the object to be classified. The results of this approach allow to see that modern image recognition techniques have shortcomings, such as errors when searching large databases, recognition errors when changing the angle of the object, effects of lighting on recognizing quality, signs of masking, and software sensitivity to facial expressions. The proposed multimodal biometric identification system should have four building blocks: a data acquisition module, a trait generation module, and an authentication algorithm. Multimodal solutions based on quantum computing can improve the stability and accuracy of biometric systems and increase their reliability in the event of unauthorized access attempts.

4.The developed model showed that the task of implementing a face recognition system based on a quantum computing algorithm ensures parallel processing of large data arrays of facial images using quantum correlation between informative features. This technology combines the foundations of quantum algorithms with classical algorithms, enabling an effective face recognition system that solves many shortcomings. Advantages of using hybrid computational algorithms for face recognition include faster computation through quantum evolutionary operators, introducing quantum operators of superposition and correlation, and radically new approaches to face recognition algorithms and cryptography and stenography algorithms. These algorithms also offer immaterial dependence on environmental interference, no dependence on stationary or moving objects or cameras, and high security when interfering with image control channels. The algorithmic model of quantum cryptography for face recognition techniques can be used independently or in conjunction with other quantum cryptographic algorithms for image and video processing.

Conflicts of Interest

The authors declare that they have no conflict of interest in relation to this research, whether financial, personal, authorship or otherwise, that could affect the research and its results presented in this paper.

Financing

The study was performed without financial support.

Data availability

The manuscript has no associated data.

Use of artificial intelligence

The authors confirm that they did not use artificial intelligence technologies when creating the current manuscript.

References

1. Tajane, K., Gomsale, A., Gomsale, A., Yadav, A., Walzade, S. (2023). Online Exam Proctoring System. International Journal of Advanced Research in Science, Communication and Technology, 3 (1), 202–207. https://doi.org/10.48175/ijarsct-9027
2. Ganar, E. S., Mohammad, S., Zohair, K., Shaikh, R. (2023). Online Exam Proctoring System. International Journal of Advanced Research in Science, Communication and Technology, 3 (5), 138–142. https://doi.org/10.48175/ijarsct-9334
3. Felsinger, D. N., Halloluwa, T., Fonseka, C. L. I. (2023). Experiences of conducting online exam proctoring in low-resource settings: a Sri Lankan case study. Information Technologies and Learning Tools, 93 (1), 163–177. https://doi.org/10.33407/itlt.v93i1.5094
4. Sharma, P. (2023). Proctoring and Monitoring-Based Examination System. International Journal for Research in Applied Science and Engineering Technology, 11 (6), 73–79. https://doi.org/10.22214/ijraset.2023.51899
5. Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D. et al. (2021). The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. Systematic Reviews, 10 (1). https://doi.org/10.1186/s13643-021-01626-4
6. Kitchenham, B., Brereton, P. (2013). A systematic review of systematic review process research in software engineering. Information and Software Technology, 55 (12), 2049–2075. https://doi.org/10.1016/j.infsof.2013.07.010
7. Barrio, F. (2022). Legal and Pedagogical Issues with Online Exam Proctoring. European Journal of Law and Technology, 13 (1). Available at: https://ejlt.org/index.php/ejlt/article/view/886
8. Baso, Y. S. (2022). Proctoring and Non-proctoring Systems. International Journal of Advanced Computer Science and Applications, 13 (6). https://doi.org/10.14569/ijacsa.2022.0130610
9. Hussein, M. J., Yusuf, J., Deb, A. S., Fong, L., Naidu, S. (2020). An Evaluation of Online Proctoring Tools. Open Praxis, 12 (4), 509. https://doi.org/10.5944/openpraxis.12.4.1113
10. Alessio, H. M., Malay, N. J., Maurer, K., Bailer, A. J., Rubin, B. (2017). Examining the Effect of Proctoring on Online Test Scores. Online Learning, 21 (1). https://doi.org/10.24059/olj.v21i1.885
11. Kolski, T., Weible, J. L. (2019). Do Community College Students Demonstrate Different Behaviors from Four-Year University Students on Virtual Proctored Exams? Community College Journal of Research and Practice, 43 (10-11), 690–701. https://doi.org/10.1080/10668926.2019.1600615
12. Conijn, R., Kleingeld, A., Matzat, U., Snijders, C. (2022). The fear of big brother: The potential negative side-effects of proctored exams. Journal of Computer Assisted Learning, 38 (6), 1521–1534. https://doi.org/10.1111/jcal.12651
13. Han, S., Nikou, S., Yilma Ayele, W. (2023). Digital proctoring in higher education: a systematic literature review. International Journal of Educational Management, 38 (1), 265–285. https://doi.org/10.1108/ijem-12-2022-0522
14. Nurpeisova, A., Shaushenova, A., Mutalova, Z., Ongarbayeva, M., Niyazbekova, S., Bekenova, A. et al. (2023). Research on the Development of a Proctoring System for Conducting Online Exams in Kazakhstan. Computation, 11 (6), 120. https://doi.org/10.3390/computation11060120
15. Hernandez-de-Menendez, M., Morales-Menendez, R., Escobar, C. A., Arinez, J. (2021). Biometric applications in education. International Journal on Interactive Design and Manufacturing (IJIDeM), 15 (2-3), 365–380. https://doi.org/10.1007/s12008-021-00760-6
16. A model of training in information security technologies in the context of globalization (2022). Certificate of entry of information into the State register of rights to objects protected by copyright of the Republic of Kazakhstan, No. 29025.
17. Deutsch, D. (1985). Quantum theory, the Church-Turing principle and the universal quantum computer. Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences, 400 (1818), 97–117. https://doi.org/10.1098/rspa.1985.0070
18. Nielsen, M. A., Chuang, I. L. (2010). Quantum Computation and Quantum Information. Cambridge: Cambridge University Press. https://doi.org/10.1017/cbo9780511976667
19. Shor, P. W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. Proceedings 35th Annual Symposium on Foundations of Computer Science. https://doi.org/10.1109/sfcs.1994.365700
20. Easttom, W. (2021). Quantum Computing and Cryptography. Modern Cryptography, 385–390. https://doi.org/10.1007/978-3-030-63115-4_19
21. Bennett, C. H. (1992). Quantum cryptography using any two nonorthogonal states. Physical Review Letters, 68 (21), 3121–3124. https://doi.org/10.1103/physrevlett.68.3121
22. Bennink, R. S., Bentley, S. J., Boyd, R. W., Howell, J. C. (2004). Quantum and Classical Coincidence Imaging. Physical Review Letters, 92 (3). https://doi.org/10.1103/physrevlett.92.033601
23. Al-Khalid, R. I., Al-Dallah, R. A., Al-Anani, A. M., Barham, R. M., Hajir, S. I. (2017). A Secure Visual Cryptography Scheme Using Private Key with Invariant Share Sizes. Journal of Software Engineering and Applications, 10 (01), 1–10. https://doi.org/10.4236/jsea.2017.101001
24. Cao, Y., Li, J., Chakraborty, C., Qin, L., Tao, L., Shao, X. (2023). Temporal Segment Neural Networks-Enabled Dynamic Hand-Gesture Recognition for Industrial Cyber-Physical Authentication Systems. IEEE Systems Journal, 17 (4), 5315–5326. https://doi.org/10.1109/jsyst.2023.3306380

25. Li, M., Yang, X., Zhu, H., Wang, F., Li, Q. (2020). Efficient and privacy-preserving online face authentication scheme. Tongxin Xuebao Journal on Communications, 41 (5), 205–214. https://doi.org/10.11959/j.issn.1000-436x.2020087
26. Zhang, X., Gonnot, T., Saniie, J. (2017). Real-Time Face Detection and Recognition in Complex Background. Journal of Signal and Information Processing, 08 (02), 99–112. https://doi.org/10.4236/jsip.2017.82007
27. Easttom, C., Ibrahim, A., Chefranov, A., Alsmadi, I., Hansen, R. (2020). Towards A Deeper NTRU Analysis: A Multi Modal Analysis. International Journal on Cryptography and Information Security, 10 (2), 11–22. https://doi.org/10.5121/ijcis.2020.10202
28. Shaller, A., Zamir, L., Nojoumian, M. (2023). Roadmap of post-quantum cryptography standardization: Side-channel attacks and countermeasures. Information and Computation, 295, 105112. https://doi.org/10.1016/j.ic.2023.105112
29. ISO/IEC 19989-2:2020. Information security – Criteria and methodology for security evaluation of biometric systems. Part 2: Biometric recognition performance. Available at: https://www.iso.org/standard/72403.html
30. Kim, B. G., Wong, D., Yang, Y. S. (2023). Quantum-Secure Hybrid Blockchain System for DID-Based Verifiable Random Function with NTRU Linkable Ring Signature. International Journal on Cryptography and Information Security, 13 (4), 01–25. https://doi.org/10.5121/ijcis.2023.13401