Journal of Theoretical and Applied Information Technology
30th June 2025. Vol.103. No.12

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

APPLICATIONS OF QUANTUM COMPUTING IN BIOMETRIC INFORMATION SECURITY

GALIYA YESMAGAMBETOVA[1], ALIMBUBI AKTAYEVA[2,*], KYMBAT SAGINBAYEVA[3], DENIS PLESKACHEV[4], ULZHAN KUSSAINOVA[5], AIDYN DAURENOVA[6], ISKANDER BAIZHANON[7], ALTYNBEK UMBETOV[8]

[1,3] Mongolian University of Science and Technology, Ulaanbaatar, Mongolia
[2,4,5,6] Department of Information systems and Informatics, A.Myrzakhmetov Kokshetau University, Kokshetau, Kazakhstan
[7]Department of Information Systems, S.Seifullin Kazakh Agro Technical Research University, Astana, Kazakhstan
[8]Department of Physics and Mathematics School, Nazarbayev Intellectual Lyceum, Almaty, Kazakhstan

E-mail: [1]gal.esm@mail.ru, [2,*]aaktaewa@list.ru, [3]skk_19739@mail.ru, [4]denispleskachv@mail.ru, [5]ulzhan-92-92@mail.ru, [6]daurenova.aa@mail.ru, [7]iskander.1.5.3@gmail.com, [8]altynbek.umbetov@gmail.com

*Authors to whom correspondence should be addressed: aakhtaewa@gmail.com

ABSTRACT

Quantum computing is based on the principles of quantum mechanics and uses quantum bits (qubits) that can exist in a state of superposition and entanglement. They promise a revolution in computing and information security. Firstly, using quantum algorithms in information technology opens up new possibilities for processing and protecting data. Secondly, biometric information security relies on a person's unique physical and behavioural characteristics, such as fingerprints, facial recognition, iris, voice, and others. These methods provide a high level of security due to their uniqueness and difficulty in counterfeiting. Combining the principles of quantum computing and biometric information security allows us to identify their similarities and integration capabilities to create reliable systems for protecting confidential information. While previous research in biometric information security has focused on individual aspects of decision-making to ensure the information security of educational institutions when using facial recognition technologies, this work presents a comprehensive framework combining several components into a single unified system for using various quantum cryptography algorithms. The main advantages of using quantum computing in object and image detection include accelerating the computational process using quantum components, robustness at different object angles, suitability for moving or static conditions, cryptographic noise immunity, and the ability to work in real practical conditions. The advantages of the quantum cryptographic scheme for face recognition technologies include ease of implementation, high cryptography security, the ability to parallelise the processes of encoding and decoding images, and the fact that complex computer equipment is not required. The study results provide a solid foundation for developing hybrid quantum computing and biometric information security technologies. Using the possibility of hybrid computing opens up new horizons for the standardisation and public dissemination of new technologies, and such a combination ensures reliable protection of confidential information and stimulates further research aimed at improving data protection methods in the context of the rapid development of the digital world.

Keywords: *Qubit, pattern recognition, quantum algorithm, multi-modal biometric technology, cybersecurity.*

1. INTRODUCTION

In recent decades, technological progress has opened up new horizons in computing and information security, and quantum computing and biometric information security have become essential aspects of data security.

Quantum computing is based on the principles of quantum mechanics and uses quantum bits (qubits) that can exist in a state of superposition and entanglement. It promises a revolution in computing technology and information security. Quantum bits, or qubits, allow quantum computers to perform complex

calculations inaccessible to modern computers' computing resources. Using quantum algorithms in information technology opens up new data processing and protection possibilities.

One of the priority areas for improving efficiency is the advancement of biometric authentication technologies, which currently play a central role in security systems. Their importance is because the human factor plays a decisive role in ensuring the stability and protection of critical elements within the management systems of educational organisations. For instance, an inefficient authentication system significantly increases the risk of unauthorised access by malicious actors to confidential information about students. Such actions may disrupt the functioning of key information infrastructures (KIIs), lead to incidents, and even jeopardise the confidential information management system of a university's educational process.

Biometric information protection, on the other hand, relies on a person's unique physical and behavioural characteristics, such as fingerprints, facial recognition, irises, voice, and others. These methods provide a high level of security due to their uniqueness and the difficulty of counterfeiting. Biometric information protection involves using a person's unique physical characteristics for authentication and authorisation. Biometric authentication is already widely used in various fields, including mobile devices, access control systems, and financial institutions.

Quantum computing and biometric information security are two cutting-edge areas that, when combined, can lead to revolutionary changes in cybersecurity. Combining quantum computing and biometric information security has the potential to create new, more reliable security systems. Nevertheless, the development and implementation of these technologies face several challenges. Quantum computing is at the active research stage and requires significant efforts to create stable and reliable quantum computer infrastructures. Biometric information protection also faces privacy issues and legal aspects of using biometric data. Improving biometric authentication tools is essential in this context, as they are integral to modern security systems.

Thus, the study of the application of quantum computing in biometric information security represents an important direction for the future of cybersecurity. The article presents a fresh look at the assessment of these technologies' current state and development prospects, as well as a discussion of their possible advantages and challenges. The article is valuable for readers because it explores various aspects of hybrid technologies, where quantum algorithms can provide faster and more accurate processing of biometric data, and quantum and post-quantum cryptography can offer new methods to protect this data from hacking and unauthorised access. In addition, from a scientific point of view, it is important to study how the combination of quantum computing and biometric information security has factors and high potential that affect the quality of new, more reliable security systems being developed. The results of this study offer a solid foundation for the future development of hybrid quantum computing and biometric information security technologies, encouraging further research, standardisation efforts, and public dissemination for further improvement.

2. LITERATURE REVIEW

We conducted a comprehensive search and statistical analysis of research papers on developing a pattern recognition algorithm for a proctoring system in an educational setting published from 1996 to 2024 (See Figure 1). As of April 30, 2024, 49 publications (consisting of 12 research articles, 34 conference proceedings, and 3 other research papers) were identified by searching the keywords “proctoring system”, “pattern recognition”, “quantum algorithm”, and “multimodal biometrics technology”.

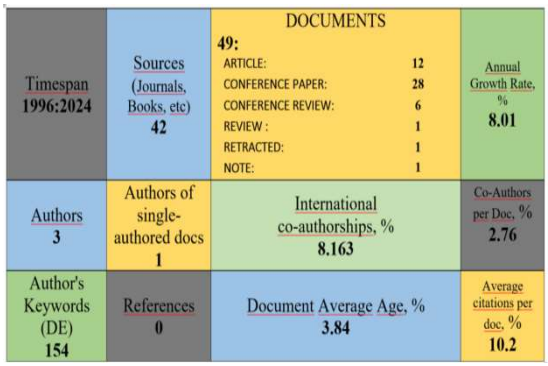

Figure 1: Statistical graph of the number of studies in different periods

As a research source, we chose the Scopus database, which is widely recognised as an authoritative source in the academic circles of researchers. The Scopus database includes a large number of high-quality articles published in major scientific journals that accept rigorous peer review systems and are widely recognised for their

quality, as well as widely covering various scientific journals with a high impact factor and containing articles that have undergone rigorous peer review, guaranteeing high quality. We searched for articles in the Scopus database. We studied the relevant literature on applying the proctoring system and the quantum pattern recognition algorithm in education's information protection field. After receiving sample articles, we carefully screened the authors, abstracts, introductions, and conclusions of the articles to eliminate content duplication, ensuring the research papers' accuracy.

The screening step includes two stages. First, duplicate items were eliminated, resulting in 49 unique articles that were moved to the next stage, where the relevance of the articles was examined based on their titles and abstracts. The second stage resulted in 40 articles for further consideration. The third step of the Prisma model is eligibility, in which the authors read the full text of articles, among which 12 were considered eligible for final review. In fact, at this stage, after reading the abstract and the full text of the articles, the articles that did not develop a model for one of the fields related to economics using the machine learning method were removed.

The last step of the Prisma model is creating a database for qualitative and quantitative analysis. The current study database comprises 12 articles, all of which have been analysed in this study. Figure 2 illustrates the steps of making the database of the present study based on the Prisma method.

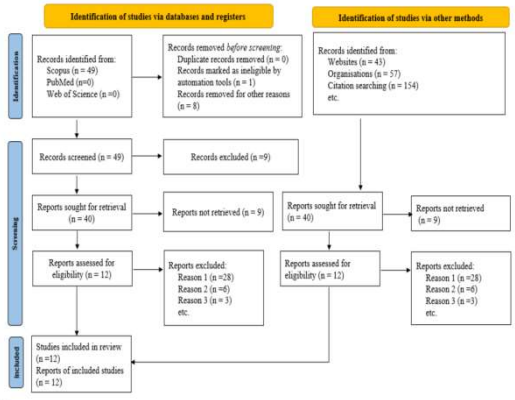

Figure 2: PRISMA 2020 flow diagram for new systematic reviews, which included searches of databases, registers and other sources

Figure 3 depicts the hierarchy of the studies' most commonly utilised terms and phrases.

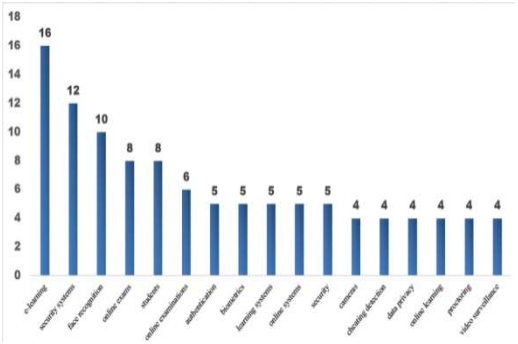

Figure 3: Ranking of the most frequently used terms and phrases

In Figure 4, high-frequency words are visually selected to help readers better understand important information. The software VOSviewer tool was used to visualise a keyword network in a Scopus database.

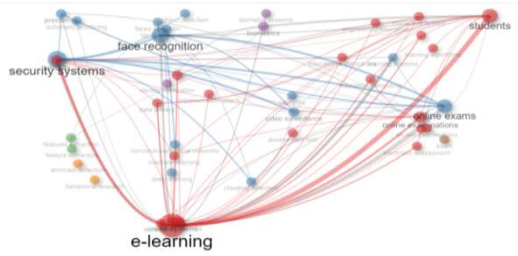

Figure 4: Results of statistical modelling of citations

After creating a word cloud (as depicted in Figure 5), we performed a cluster analysis of keywords using relevant articles in the Scopus database.

Figure 5: Word cloud of all searched papers (higher frequency words are displayed horizontally or vertically in larger font)

As a result, 12 high-quality scientific papers from the Scopus databases were identified as the literary base for this study (see Figure 6). In addition, 28 works directly devoted to the infrastructure of proctoring systems make up 65% of the total.

Figure 6 shows the percentage of study keywords in the set of papers included in this study. The visual connections between the nodes reflect their co-occurrence in research publications, with each node representing a single keyword. The size of the nodes indicates the frequency of these terms, while the thickness of the connecting lines demonstrates the strength of their relationship. This study's keywords, such as "biometrics, security system and e-learning", are the most prominent nodes.

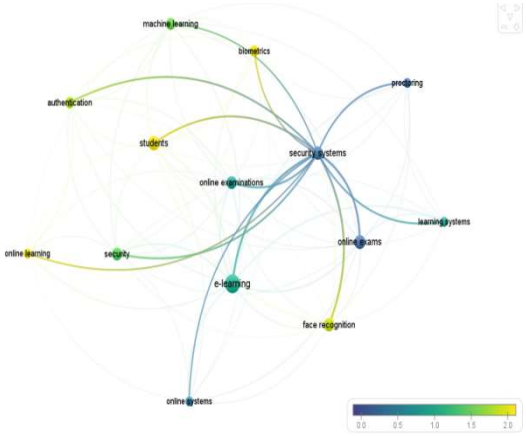

Figure 6: Percentage of different types of studies

The statistical analysis method was also used to calculate the number of works from 1996 to 2023 and clearly present the results as statistical graphs. Figure 7 clearly shows that in the period 2021–2023, the number of studies has peaked. In the previous almost twenty years, the number of scientific papers on research in this area showed a gradual downward trend.

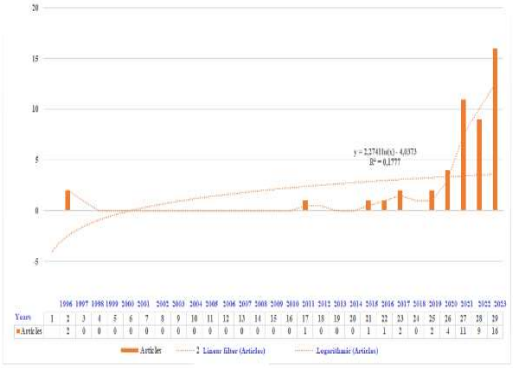

Figure 7: Number of articles published between 1996 and 2023 (through April 30, 2024)

This statistical result can provide valuable information for analysing the historical context of trends in developing research on information protection proctoring systems in education [2].

This paper [3] proposes a method for two-factor authentication using quantum-generated one-time passwords (QOTP) and user biometrics for identification. Two-factor authentication using one-time passwords (OTP) is widely used for online transactions. Still, it faces security threats due to the static nature of shared secrets and the predictability of OTP generation. Classical computing methods have vulnerabilities that can be mitigated with quantum technologies.

In this paper [4], a quantum multi-factor authentication mechanism is presented based on the complexity problem of quantum communication with hidden correspondences. It proposes step-by-step graded authentication for users using a quantum token.

This article [5] presents a new three-factor quantum identity authentication scheme consisting of two phases: registration and login/authentication. It applies two layers of quantum encryption for the voice signal, using simple quantum circuits and various pseudorandom keys. The server stores the encrypted client voice data and uses quantum Euclidean distance to compare it with previously saved data during authentication. According to the authors, the scheme ensures secure processing, transmission, and data storage, guaranteeing protection against attacks, real-time communication, and the efficient use of quantum technologies.

Many studies highlight that current methods of protecting information using biometric data are ineffective against attacks by

frontmen because they require substantial resources and often lack accuracy when analysing biometric features. Also, not enough attention is paid to fully combining these methods with authentication techniques that use quantum computing, which could offer a new way to create a random quantum cryptographic key based on the fingerprints of the sender and recipient.

3. METHODOLOGY AND RESULTS

3.1 Basic principles of quantum computing

Quantum computing is a new paradigm in computing technologies based on the fundamental principles of quantum mechanics. Unlike classical computers that operate with bits, quantum computers use qubits (quantum bits). Qubits have the unique ability to be in a state of superposition, which allows them to represent both 0 and 1 simultaneously. This dramatically increases computing power, allowing quantum computers to perform many calculations in parallel.

Another important characteristic of quantum computing is quantum entanglement. Entanglement allows a qubit to be in a special interconnected state, in which a change in the state of one qubit instantly affects the state of another, regardless of the distance between them. This property dramatically increases the possibilities of data processing and information transfer.

Quantum algorithms such as Shor's algorithm for factoring integers and Grover's algorithm for searching in disordered databases demonstrate the superiority of quantum computers over classical ones in solving certain problems. However, current quantum computers have not yet reached the required level of stability and scalability, which remains a major challenge for developers.

The development of quantum computing promises significant changes in cryptography, chemical process modelling, optimisation, and artificial intelligence. Research and development continue, and with each step, scientists are getting closer to creating practical and powerful quantum computers capable of solving problems inaccessible to modern classical computers.

A system of two qubits can be in a state where measuring one qubit immediately determines the state of the other. This state describes a system in which measuring one qubit immediately determines the state of another qubit. This principle underlies quantum entanglement, which makes it important for quantum computing and technology. Table 1 shows the basic formulas and principles of protecting confidential information using quantum computing.

Table 1: Basic formulas and principles for protecting confidential information using quantum computing

S. No	Title	Basic formulas and principles
Principles of superposition and entanglement		
1	Superposition	$\|\psi\rangle = \alpha\|0\rangle + \beta\|1\rangle$, where $\|\psi\rangle$ is the state of the qubit, α and β are complex coefficients satisfying the normalisation condition: $\|\alpha\|^2 + \|\beta\|^2 = 1$
2	The principle of superposition of states	$\psi_3 = c_1\psi_1 + c_2\psi_2$, superposition of states $\psi_1$and ψ_2.
3	Entanglement	$\|\psi\rangle = \frac{1}{\sqrt{2}}(\|100\rangle + \|11\rangle)$
4	Measuring a qubit	$\|\psi\rangle_{AB} = \sum_{i,j} c_{i,j}\|i\rangle_A \otimes \|j\rangle_B$ - where a system of two qubits can be in a state where measuring one qubit immediately determines the state of the other.
The principle of quantum key distribution (QKD)		
1	BB84 protocol	Alice sends a sequence of qubits to Bob. 1. Each qubit is randomly selected from four basic states 2. For example, ($\|\mathbf{0}\rangle, \|\nearrow\rangle \frac{\mathbf{1}}{\sqrt{2}}(\|\updownarrow\rangle + \|\leftrightarrow\rangle)$, $\|\mathbf{1}\rangle, \|\nwarrow\rangle = \frac{\mathbf{1}}{\sqrt{2}}(\|\updownarrow\rangle - \|\leftrightarrow\rangle)$ 3. Bob measures each qubit in one of two bases. 4. Alice and Bob exchange information about the bases through a public channel and discard inconsistent results.
2	To identify erroneous characters in bits, you can use the ratio	$e = \frac{(\text{Erroneous bits})}{\text{all bits}}$ - the formula shows the ratio of the number of erroneous bits to the total number of bits in the system. It is used to estimate errors in data transmission or calculations.

The principle of Shor's quantum algorithm. Factoring a number is one of the key tasks that Shor's algorithm can solve. Shor's algorithm uses the quantum Fourier transform (QFT) to find the periodicity of a function and, ultimately, to decompose the number N into two prime factors. The primary step of the Shor algorithm can be expressed in terms of the

quantum Fourier transform. For example, initialising the status register [6]:

1. Start with the state $|0\rangle^{\otimes n}$.
2. A discrete logarithm is used to check the U_f operation for the state of the register.
3. Application of the QFT:
4. Apply QFT to the register to find the period, then the QFT formula for Shor's algorithm is:

$$QFT: |j\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i jk/N} |k\rangle \qquad (1)$$

This formula describes how the state $|j\rangle$ is transformed into a superposition of states $|k\rangle$ with coefficients $e^{2\pi ijk/N}$, with coefficients $\frac{1}{\sqrt{N}}$. The quantum Fourier transform is a key component in quantum computing algorithms, such as Shor's algorithm, for factoring numbers.

Eventually, after applying QFT, we can measure the register and use classical methods to find the prime factors of N. Shor's algorithm. This shows how quantum computing can solve some problems much faster than classical algorithms.

Grover's quantum algorithm principle and unsorted database search. Grover's quantum algorithm, proposed by L. Graver in 1996, is one of the key quantum computing algorithms, providing a quadratic acceleration of searching in an unsorted database compared to classical methods. Grover's algorithm demonstrates how quantum effects such as superposition and interference can be used to solve optimisation and search problems.

In the classical case, searching for a target element in an unsorted database of N elements requires, on average, O(N) operations (iterating through all the elements). Grover's algorithm reduces this time to O(√(N)) quantum operations, which provides significant acceleration for large (N). The mathematical model of the basic steps of Grover's quantum algorithm can be described as follows [7]:

1. Initialisation of a superposition. The quantum register is initialised in a uniform superposition of all possible states. For $N = 2^n$ qubits, this corresponds to:

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{X=0}^{N-1} |x\rangle \qquad (2)$$

2. Oracle is a quantum U_{oracle} operation that "marks" the target state$|x0\rangle$ by changing its phase (for example, multiplying the amplitude by -1). This is expressed as:

$$U_{oracle}|x\rangle = -1^{f(x)} \Big| x\rangle, \; f(x) = \begin{cases} 1, x = x_0 \\ 0, else. \end{cases} \qquad (3)$$

3. The inverse of the average. An operation that increases the amplitude of the marked state by decreasing the amplitudes of the others. This is achieved by converting:

1. First, the Hadamard matrix is applied to all qubits.
2. Then, the sign of all amplitudes is inverted, except for the amplitude of the state $|0\rangle$.
3. Hadamard matrices are applied again.
4. Mathematically, this transformation can be written as:

$$U_{diff} = 2|\psi\rangle|\psi\rangle - I \qquad (4)$$

where
$|\psi\rangle$ - a uniform superposition, and I is a unit matrix

5. Repeat steps 2 – 3. The oracle and inversion operations relative to the mean are repeated approximately $\pi/4\sqrt{(N)}$ times. After that, measuring the register will likely give the target state $x[[\hat{}]] \dashv \_0|x_0\rangle$. Table 2 shows the advantages and disadvantages of Grover's algorithm. Grover's algorithm for quantum computing illustrates the power of quantum methods in optimisation and search tasks. It's confirms that even moderate quantum acceleration can dramatically change approaches to solving practical problems such as big data analysis, machine learning, and cryptography.

Table 2: Advantages and disadvantages of Grover's algorithm

S. No	Principles	Description
Advantages of the Grover algorithm:		
1	Quadratic acceleration	The efficiency of (O($\sqrt{(N)}$) versus (O(N)) in the classical case.
2	Versatility	It is applicable for searching and solving problems that come down to search (for example, finding collisions of hash functions, optimisation).
3	Cryptography Applications	It can be used to attack symmetric ciphers (Example, to speed up key sorting).
Limitations		
1	Non-exponential acceleration	Unlike Shor's algorithm, which accelerates factorisation, Grover's algorithm provides only a quadratic improvement.
2	Dependence on the oracle	Efficiency requires a "black box" (oracle) to label target states.

3	Data structure requirement	The algorithm does not consider the possible data structure, which limits its applicability in some scenarios.

However, its implementation requires error-resistant quantum computers, which remains a technological challenge. The principle of Grover's quantum algorithm allows you to find the label of the desired element in an unsorted database of N elements in O(sqrt{N}) steps, which is significantly faster than the classical O(N) approach. The main idea of the algorithm is amplitude amplification. Verification of quantum entanglement violating Bell inequalities:

$$E(a,b) = \langle A(a)B(b)\rangle = \sum_{a,b} abP(a,b) \quad (5)$$

where
E(a, b) - the expected value of the measurement products on two quantum entangled particles. The above formulas and principles provide a framework for understanding how quantum computing can be used to protect confidential information [8].

3.2 Biometric information protection

Biometric information protection includes using a person's unique physical characteristics, such as fingerprints, facial recognition, iris, and voice. These methods provide a high level of security, as biometric data is difficult to tamper with or steal. Biometric information security uses various mathematical and statistical methods to ensure the accuracy and reliability of authentication. Table 3 shows some of the basic formulas used in biometric protection [9, 10].

The Gaussian function, also known as the normal distribution function, is widely used to model the distribution of biometric data such as height, weight, fingerprints and other characteristics. This is because many biometric parameters tend to have a normal distribution, where most values are concentrated around the average, and extreme values are less common.

Table 3: Basic formulas used in biometric protection

S. No	Basic Formulas	Description
1	The Euclidean distance	The Euclidean distance is often used to measure the similarity between two biometric patterns. $d(x,y) = \sqrt{\sum_{i=1}^{n}(x_i - y_i)^2}$ Where d(x,y) is the distance between points x and y in n-dimensional space, and x_i and y_i are the coordinates of these points
2	Correlation coefficient	The correlation coefficient measures the degree of linear relationship between two datasets. It shows how strongly the variables x and y are related. A high r value indicates a strong correlation, which is important for assessing the similarity of biometric data.
3	Pearson correlation coefficient	In the case of the Pearson correlation coefficient, the formula looks like this: $r = \frac{\sum(x_i - x)(y_i - y)}{\sqrt{(x_i - x)^2 \sum(y_i - y)^2}}$ Where x_i and y_i are the values of variables x and y. {x} and {y} are the average variables x and y values. The values of the correlation coefficient r range from -1 to 1, where r = 1 indicates an ideal positive linear relationship. r = -1 indicates an ideal negative linear relationship. r = 0 indicates that there is no linear relationship.

The formula gives the density function of the normal distribution (Gaussian function):

$$f(x) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(x-\mu)^2}{2\sigma^2}} \quad (6)$$

where
x - a variable (for example, the value of a biometric parameter).
μ - the mathematical expectation (the average value of the distribution).
σ - the standard deviation (a measure of the spread of data around the average).
σ^2 - the variance.
ε - the base of the natural logarithm (approximately e = 2.71828).

Properties of the Gaussian function:
1. *Symmetry:* The function is symmetric with respect to the average value of μ.
2. *Bell shape:* The function graph has a bell shape, with the peak at the point χ = m.
3. *Area under the curve:* The area under the curve of the normal distribution is 1, which corresponds to a 100 % probability.
4. *Rule*:
a) About 68 % of the data lies within one standard deviation from the mean (μ ± σ),
b) About 95 % of the data lies within two standard deviations (μ ± 2σ),

c) About 99.7 % of the data lies within three standard deviations ($\mu \pm 3\sigma$).

Examples of applications in biometric's:

1. Data modelling: The Gaussian function describes the distribution of biometric parameters such as height, weight, step length, and others.
2. *Classification and identification:* In biometric identification systems (for example, face or fingerprint recognition), a normal distribution helps to assess the probability of data belonging to a certain class.
3. *Noise filtering:* Gaussian filters smooth data and removes noise in biometric signal processing.

Example 1: If we consider the height of people in a population, then the average value of m can be, for example, 170 cm, and the standard deviation of s is 10 cm. Most people will have a height in the range of 160-180 cm (within ($\mu \pm \sigma$)), and extreme values (for example, 140 cm or 200 cm) will be rare. Thus, the Gaussian function is a powerful tool for analysing and modelling biometric data.

The Bayesian classifier for biometric data protection is a powerful decision-making tool based on a probabilistic approach that is widely used in biometric data protection tasks. With the growing threats associated with unauthorised access to personal information, using methods based on probability theory is becoming especially relevant to ensure reliable authentication and identification of users. The Bayesian classifier is based on Bayes' theorem, which makes it possible to estimate the a posteriori probability of biometric data belonging to a certain class (for example, "authorised user*"* or "attacker") based on observed features. Formally, this is expressed as follows:

$$P(C|X) = (P(X|C)) * \frac{P(C)}{P(X)} \quad (7)$$

where

$P(C|X)$ - the a posteriori probability of class C, given the observed features of X.

$P(X|C)$ - the likelihood, that is, the probability of observing features XX under the condition of class C.

$P(C)$ - a priori probability of class C.

P(X) - a normalising constant representing the probability of observing features of X.

Biometric data, such as fingerprints, irises, voice samples, or facial images, are highly unique, making them an effective tool for identifying individuals. However, their use is also associated with risks of leakage and forgery (see Table 4).

Table 4: The advantages of limiting the Bayesian approach

S. No	Name	Description
Advantages of the Bayesian approach		
1	Accounting for uncertainty:	Probability-based solutions are easy to interpret and analyse, which is important for developing reliable protection systems.
2	Adaptability:	The classifier can be adapted to changing conditions, for example, when new types of attacks appear.
3	Interpret ability:	Probability-based solutions are easy to interpret and analyse, which is important for developing reliable protection systems.
Limitations		
1	Dependence on data quality:	The classifier's accuracy depends on the training data quality and misrepresentations.
2	The assumption of feature independence:	The naive Bayesian model assumes conditional feature independence, which may not be fulfilled in real-world tasks.
3	Computational complexity:	For multidimensional data, calculating likelihood can be computationally expensive.

The Bayesian classifier is an effective tool for protecting biometric data and providing reliable authentication and user identification. Its ability to consider probabilistic dependencies and adapt to changing conditions makes it an important component of modern biometric security systems. Further research may improve classification accuracy by considering correlations between features and integrating them with other machine-learning methods [11]. The Bayesian classifier allows you to solve the following tasks:

1. *User authentication:* The probability of the submitted data belonging to an authorised user is calculated based on biometric features. The decision is made by comparing the a posteriori probability with a given threshold.
2. *Anomaly detection:* The Bayesian classifier can be used to identify suspicious activities, such as attempts to fake biometric data. Anomalies are identified based on the low probability that the observed data correspond to a normal distribution.
3. *Classification of threats:* In biometric data protection systems, the classifier allows you to separate requests into legitimate and potentially

dangerous ones. For example, facial recognition systems can distinguish real faces from photographs or masks.

Example 2. Consider a facial recognition system where a Bayesian classifier determines whether a presented image matches a registered user. At the training stage, the model evaluates the distribution of features (for example, the distances between key points of the face) for each user. At the classification stage, the probability is calculated that the new image belongs to an authorised user, and a decision is made to grant access.

Biometric authentication is one of the most advanced methods of ensuring security. It is based on a person's unique physical and behavioural characteristics. These methods include fingerprints, facial recognition, iris, voice, and other biometric features that provide high accuracy and reliability. To maximise the effectiveness of biometric authentication, various methods and algorithms are used to increase reliability and accuracy (see Tables 5 and 6).

Table 5: Methods for improving reliability and accuracy

S. No	Method	Explanation
1	Feature extraction:	One key step of biometric authentication is extracting unique features from biometric data. This may include analysing textures, contours, or other unique characteristics. In the case of face recognition, for example, methods are used to detect and highlight key points of the face, such as the corners of the eyes, the tip of the nose, and the corners of the mouth. These attributes are then converted into numeric vectors, which are used for comparison and authentication.
2	Normalisation of data:	Normalisation of biometric data is necessary to reduce the influence of external factors such as lighting, posture, image quality, or acoustic conditions. This process involves converting the data into a standardised format, which improves its consistency and accuracy. For example, normalisation may include image alignment and smoothing for fingerprints.
3	Comparing Templates:	Biometric patterns are compared using various algorithms, such as correlation methods, Euclidean distance, histograms, and neural networks. These algorithms allow you to assess the degree of similarity between two biometric patterns and determine whether they correspond to each other. For example, correlation methods allow you to compare texture patterns on fingerprints.
4	Threshold values:	Setting thresholds is a critical aspect of biometric authentication. The thresholds determine the acceptable degree of similarity between the templates for successful authentication. The thresholds are optimised to minimise errors of the first kind (false accept rate - FAR) and the second kind (false reject rate - FRR). Setting the thresholds correctly allows you to balance the system's security and ease of use.
5	Signal filtering and processing:	Filtering and signal processing methods improve the quality of the input data. For example, filters can eliminate noise and enhance signal clarity when analysing biometric voice data. Similarly, contrast and detail enhancement techniques can be used for images.

These methods and approaches allow us to ensure biometric authentication systems' high reliability and accuracy. They contribute to improving system performance and security, making them more efficient and reliable.

Table 6: Methods for evaluating and improving performance

S. No	Method	Content
1	Error evaluation:	The performance of biometric authentication systems is assessed based on two leading error indicators: False Accept Rate (FAR) and False Reject Rate (FRR). The FAR indicates the frequency of false positives when the system improperly accepts an unauthorised user. In contrast, the FRR indicates the frequency of false rejections when the system improperly rejects an authorised user. These indicators allow you to evaluate the system's effectiveness and reliability and serve as the basis for its improvement.

2	Cross-validation:	Cross-validation is a standard method for evaluating the accuracy of biometric authentication models. This method involves dividing the data into training and test sets to test the model on new data that was not used in the training process. Cross-validation allows you to evaluate the model's generalising ability and identify possible retraining problems.
3	Adaptive algorithms:	Adaptive algorithms can be adjusted depending on changes in users' biometric data. This is especially important for characteristics such as appearance or voice that can change over time. Adaptive algorithms ensure the system's long-term accuracy and increase its resilience to data variations.
4	Regular data updates:	Regular updating of users' biometric data is an important aspect of maintaining the relevance and accuracy of the templates. This is especially important for dynamic biometric features such as voice, which can change over time. Data updates allow the system to adapt to changes and maintain high accuracy.
5	Testing on different samples:	Testing the system on various data samples helps assess its resistance to variation and generalisation. This allows you to identify possible system vulnerabilities and take measures to eliminate them. The diverse data samples may include data from different demographic groups, lighting conditions, acoustic conditions, and other factors affecting biometric authentication.

3.3 Combining methods and principles of quantum computing and biometric information security

Applying quantum computing to biometric security can significantly improve biometric information security. For example, quantum algorithms can recognise biometric data faster and more accurately. Quantum cryptography, based on the principles of quantum mechanics, can provide a higher level of security for transmitting and storing biometric data. Quantum networks can provide secure communication channels for the transmission of biometric data. Combining the formulas and principles of quantum computing and biometric information protection makes it possible to identify their similarities and integration possibilities for creating reliable security systems (see Table 7).

Table 7: Combining formulas and principles of quantum computing and biometric security

S. No	Description of the principles of quantum computing and biometric information security	Formulas
Basic formulas of quantum computing		
1	Superposition is a key resource for implementing quantum algorithms, but its practical use requires noise reduction and precise control of quantum states.	$\|\psi\rangle = \alpha\|0\rangle + \beta\|1\rangle$ where $\|0\rangle$ и $\|1\rangle$ are orthonormal basis states (for example, spin up/down or photon polarisation). $\alpha, \beta \in C$ amplitudes of probability satisfying the normalisation condition: $\|\alpha\|^2 + \|\beta\|^2 = 1$
2	Entanglement is a major resource for quantum technologies, providing security, computational speed, and measurement accuracy advantages. However, its practical use requires overcoming engineering and physical barriers related to the conservation and control of quantum states.	$\|\psi\rangle = \frac{1}{\sqrt{2}}\|00\rangle + \|11\rangle$ where two qubits are in the most entangled state. Quantum entanglement is a phenomenon in which the states of two or more particles become inseparable, even with spatial separation.
3	Quantum key distribution (QKD) is used to secure cryptography key transmission. This technology evaluates the probability of error to ensure the security and reliability of the transmitted data.	$e = \frac{\text{erroneous bits}}{\text{all bits}}$ where erroneous bits\text {erroneous bits} is the number of bits that were transmitted incorrectly. All bits\text{all bits} - the total number of transmitted bits.
4	The quantum four-handed Fourier transform (QFT) is an essential algorithm in quantum computing. It transforms quantum states.	$QFT: \|j\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i j k / N} \|k\rangle$ where $\|j\rangle$ is the initial quantum state N is the number of states. $\sum$ is the sum overall k from 0 to N-1. $e^{2\pi i j k / N}$ is the phase multiple.
Basic formulas for biometric information protection		

1	The Euclidean distance measures the distance between two points x and y in non-dimensional space. It is often used in biometric systems to compare biometric patterns such as fingerprints, facial images, and other data.	$d_{pq} = \sqrt{\sum_{i=1}^{n}(p_i - q_i)^2}$
2	The correlation coefficient measures the degree of linear dependence between two variables, x and y. The r value ranges from -1 to 1, where -1 means a complete negative linear relationship, 1 means a complete positive linear relationship, and 0 means no linear relationship.	Correlation coefficient: $r_{xy} = \frac{\sum(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum(x_i - \bar{x})^2(y_i - \bar{y})^2}}$
3	The Gaussian function is used to model the distribution of various data types, including biometric data. The normal distribution is often used because of its versatility and mathematical properties.	$f(x) = \frac{1}{\sqrt{(2 * \pi * \varsigma^2)}} * e^{(-\frac{(x-\mu)^2}{2*\varsigma^2})}$
4	The Bayesian classifier calculates the a posteriori probability of class C_i under the condition of the observed feature xx. It is based on Bayes' theorem and helps classify objects into different categories based on probabilistic estimates.	$P(A\|B) = \frac{P(B\|A)P(A)}{P(B)}$

The combination of quantum computing and biometric information protection is based on the general principles of using probabilistic and statistical methods, optimising data processing and ensuring high reliability and security (See Table 8). Integrating these technologies has significant potential to develop more powerful and secure authentication and data protection systems [23].

As the comparison with traditional methods shows, the combined methods and principles of quantum computing and biometric information protection show that traditional methods of biometric protection include the use of classical cryptography algorithms and communication networks. These methods have certain limitations in terms of speed and security.

Table 8: Combining formulas and principles of quantum computing and biometric security

№	Methods	Content
1	Principles of probability and statistics:	Both fields use probabilistic and statistical methods. In quantum computing, this is expressed through quantum states and probability distributions (superposition and entanglement), and in biometric protection, through methods such as correlation coefficients, Gaussian functions, and a Bayesian classifier.
2	Optimisation of data processing:	Both quantum computing and biometric information security strive to process large amounts of data efficiently. In biometrics, quantum algorithms (FFT - fast Fourier transform) and dimensional reduction methods (PCA - Principal Component Analysis and LDA - Linear Discriminant Analysis) aim to optimise calculations and accuracy.
3	Cryptography and Authentication:	Both areas focus on ensuring data transmission and storage reliability and security. In quantum computing, this is achieved through quantum cryptography and biometric protection through the use of unique biometric features and appropriate authentication algorithms.
4	Mathematical methods to improve accuracy:	Both fields actively use mathematical methods and formulas to improve accuracy and reliability. In quantum computing, this is represented by algorithms such as Shor and Grover, and in biometrics, it is defined by methods such as Euclidean distance and probabilistic models.

Any cryptography key must be generated in such a way that it is challenging to guess, and the process of its management does not create additional costs for users. This study addresses these issues and proposes a new method for generating a random quantum cryptography key based on the biometric data of the sender's and recipient's fingerprints. Developing a key revocation algorithm also eliminates the limitations associated with the irreversibility of biometric features. Moreover, the proposed solution eliminates the need to store the key until the moment of communication, which increases the level of security and allows for generating unique keys for different sessions. The proposed quantum cryptobiometric system is resistant to

many attacks, including known-key attacks, replay attacks, and man-in-the-middle attacks. Thus, the developed method efficiently generates a session cryptography key for secure message transmission in an unsecured network channel.

Quantum computing offers significant advantages, such as the ability to process large amounts of data in real-time and a high degree of protection against attacks. Unlike classical cryptography, quantum cryptography is virtually impossible to crack, making it more reliable for protecting biometric data.

4. DISCUSSION

Nevertheless, some specific challenges and issues need to be addressed. Firstly, quantum computing is in the early stages of development, and many aspects of this technology have yet to be explored and improved. For example, building stable and reliable quantum computers requires significant effort and investment. Secondly, using quantum algorithms for biometric information protection may require significant changes in infrastructure and software. This may include adapting existing systems and developing new security protocols.

In addition, the ethical and legal aspects of using biometric data must be considered. Privacy and personal data protection issues are becoming increasingly relevant in light of the growing use of biometric authentication methods. Clear regulations and standards are required to ensure data security and confidentiality. This discussion highlights the importance of further research and development in quantum computing and biometric information security and the need to address emerging issues and challenges.

5. LIMITATION

This study aims to assess the possibility of using quantum cryptography algorithms in face recognition systems utilised by educational institutions to manage the educational process. Applying these algorithms in proctoring technologies, which classify student images, receives particular attention. Educational institutions process and store vast amounts of confidential information about students and employees, which makes security and privacy concerns especially prominent when implementing electronic monitoring systems.

The study's results demonstrate the potential of using quantum cryptography algorithms within the context of the tasks examined. However, the obtained data has certain limitations, particularly concerning the security and privacy assurances needed for implementing electronic monitoring systems in educational settings.

Future studies should focus on examining the vulnerabilities in the security features of various technologies, such as hybrid quantum computing and biometric authentication systems. The outcomes will enable us to evaluate the resilience of these solutions against potential threats.

A promising area of exploration involves leveraging concepts from artificial neural networks in hybrid quantum computing and biometric authentication systems to enhance threat and vulnerability analysis. Such technologies can ensure a higher level of objectivity in risk assessment and improve the effectiveness of preventive measures employed by educational institutions in managing the educational process.

Secondly, the analysis focused on articles and reviews published in English and indexed in Scopus. Although this approach provides access to moderate- and high-quality publications on the topic under consideration, it also limits the scope of the study. A lack of integration with other databases and publications in different languages, such as Arabic, Chinese, or Spanish, may affect the analysis results. This gap can be filled in the future by expanding the bibliometric study to include non-English data sources that complement Scopus.

In future studies, we need to examine the weaknesses in the security features of different technologies, such as hybrid quantum computing and biometric authentication systems. The results will allow us to assess the degree of resistance of such solutions to potential threats.

A promising area involves using ideas from artificial neural networks in hybrid quantum computing and biometric authentication systems to better analyse threats and weaknesses. Such technologies can ensure a higher level of objectivity in risk assessment and improve the effectiveness of preventive measures used by educational institutions to manage the educational process.

6. CONCLUSIONS

Quantum computing and biometric information security are important cybersecurity

tools. Their integration can lead to significant improvements in data protection and authentication. Quantum computing provides new opportunities for fast and accurate recognition of biometric data, and quantum cryptography offers high security in transmitting and storing information. Research and development prospects of these technologies emphasise their potential and importance for the future of cybersecurity.

Although there are challenges, such as high costs and complexity of implementation, these technologies promise to create more reliable and effective data protection systems. Their development is especially relevant in the era of digital threats and cyber attacks. Continuous research and investments in quantum computing and biometric information security will help counter sophisticated cyber threats, ensuring high security and confidentiality. Possible breakthroughs in these areas are expected to significantly change the cybersecurity landscape in the coming years, providing more data protection and privacy. Thus, the combination of quantum computing and biometric information security represents a promising area for future cybersecurity innovations, and its potential is undeniable. It is important to continue researching and investing in developing these technologies to counter increasingly sophisticated cyber threats and ensure protection in the digital world.

REFERENCES:

[1] M. J. Page, J.E. J.E. McKenzie, P.M. Bossuyt, I. Boutron, T.C. Hoffmann, C.D. Mulrow, "The PRISMA 2020 statement: an updated guideline for reporting systematic reviews", *BMC,* vol.372(71), 2020, https://doi.org/10.1186/s13643-021-01626-4

[2] B. Kitchenham, P. Brereton, "A systematic review of systematic review process research in software engineering Information and software technology", vol.55(12), 2013, pp.2049-2075, https://doi.org/10.1016/j.infsof. 2013.07.010

[3] Sharma, Mohit & Nene, Manisha, "Two-factor authentication using biometric based quantum operations", *Security and Privacy,* 2019, pp.1-21, https://doi.org/10.1002/spy2.102

[4] Murray, H., Malone, D., "Quantum Multi-factor Authentication", *Emerging Technologies for Authorization and Authentication", ETAA 2021. Lecture Notes in Computer Science*, vol. 13136, 2021, pp.50-67, https://doi.org/10.1007 /978-3-030-93747-8_4

[5] Abdelfatah, Roayat., "Robust biometric identity authentication scheme using quantum voice encryption and quantum secure direct communications for cybersecurity", *Journal of King Saud University - Computer and Information Sciences.* Vol.36(4):102062, 2024, https://doi.org/10.1016/j.jksuci.2024.102062

[6] P.W.Shor, "Algorithms for quantum computation: discrete logarithms and factoring", *Foundations of Computer Science 1994 Proceedings 35th Annual Symposium*, pp.124-134. https://doi.org/10.1109/SFCS.1994. 365700

[7] Yesmagambetova, G., Aktayeva, A., Kubigenova, A., Ismukanova, A., Fomichyova, T., Zhartanov, S., & Daurenova, A. "Development of quantum computing algorithm of technology for monitoring learning results", *Eastern-European Journal of Enterprise Technologies*, vol.3(2(129), 2024, pp.69-82. https://doi.org/10.15587/1729-4061.2024. 306968

[8] Bennett, C. H., & Brassard, G. "Quantum cryptography: public key distribution and coin tossing", *Int. Conf. Computers, Systems & Signal Processing, 1984*, pp.175-179. https://doi.org/10.1103/PhysRevLett.68.3121

[9] S. Ryan Bennink, J. Sean Bentley, W. Robert Boyd, and John C. Howell "Quantum and classical coincidence imaging", *Phys. Rev. Letter* vol.92, 2004, pp.1-4, https://doi.org/10.1103/PhysRevLett.92.069901

[10] Fernando Barrio, "Legal and Pedagogical Issues with Online Exam Proctoring European", *Journal of Law and Technology,* vol.13(1), 2022. https://ejlt.org/index.php/ejlt/article/ view/ 886

[11] Y.S. Baso, "Proctoring and non-proctoring systems. A comparative study of online exam scores for an Arabic translating course", *International Journal of Advanced Computer Science and Applications,* vol. 13 (6), 2022, pp. 75-82, https://doi.org/10.14569/IJACSA.2022. 0130610

[12] Mohammed Juned Hussein et al., "An Evaluation of Online Proctoring Tools", *Open Praxis*, vol. 12(4), 2020, pp. 509-525, https://dx.doi.org/10.5944/openpraxis.12.4.1113

[13] Alessio, H. M., Malay, N., Maurer, K., Bailer, A. J., & B. Rubin, "Examining the effect of proctoring on online test scores", *Online Learning*, vol. 21(1), 2017, pp.146-161, https://doi.org/10.24059/olj.v21i1.885

[14] Kolski Tammi, L. Jennifer Weible, "Do Community College Students Demonstrate Different Behaviors from Four-Year

University Students on Virtual Proctored Exams", *Community College Journal of Research and Practice,* vol.43, Issue 10-11, 2019. https://doi.org/10.1080/10668926.2019.1600615

[15] Conijn R., Kleingeld A., Matzat U. and C. Snijders, "The fear of Big Brother: The potential negative side effects of proctored exams", *Journal of Computer Assisted Learning*, vol. 38(6), 2022, pp.1521-1534, https://doi.org/10.1111/jcal.12651

[16] S. Han, S. Nikou and W. Yilma Ayele, "Digital proctoring in higher education: a systematic literature review", *International Journal of Educational Management,* vol. 38(1), 2024, pp. 265-285, https://doi.org/10.1108/IJEM-12-2022-0522

[17] "A model of training in information security technologies in the context of globalisation, Certificate of entry of information into the State register of rights to objects protected by copyright of the Republic of Kazakhstan", No. 29025, dated September 26, 2022.

[18] A. Nurpeisova, A. Shaushenova, Z. Mutalova and et al., "Research on Developing a Proctoring System for Conducting Online Exams in Kazakhstan", *Computation*, vol.11(6), 2023. https://doi.org/10.3390/ computation11060120

[19] M. Hernandez-de-Menendez, R. Morales-Menendez, C.A. Escobar et al., "Biometric applications in education", *International Journal Interact Des Manuf*, 2021, pp.365-380, https://doi.org/10.1007/s12008-021-00760-6

[20] I. Al-Khalid Rola, A. Al-Dallah Randa, M. Al-Anani Aseel, M. Barham Raghad, I. Hajir Salam, "A Secure Visual Cryptography Scheme Using Private Key with Invariant Share Sizes", *Journal of Software Engineering and Applications* vol. 10(1), 2017. https://doi.org/10.4236/jsea.2017. 101001

[21] M. Li, X. Yang, H. Zhu, F. Wang, Q. Li, "Efficient and privacy-preserving online face authentication scheme", *Tongxin Xuebao Journal on Communications*, vol.41(5), 2020, pp.205-215, https://doi.org/10.11959/j.issn.1000-436x.2020087

[22] C. Easttom, An. Melhem, A. Chefranov, I. Alsmadi, and R. Hansen, "Towards A Deeper NTRU Analysis: A Multimodal Analysis", *International Journal on Cryptography and Information Security*, vol.10(2), 2020, pp.11-22, https://doi.org/10.5121/ijcis.2020.10202

[23] B. Kim, D. Wong, Y. Yang, "Quantum-Secure Hybrid Blockchain System for DID-Based Verifiable Random Function with NTRU Linkable Ring Signature", *International Journal on Cryptography and Information Security*, vol.13, 2023, pp.01-25, https://doi.org/10.5121/ ijcis.2023.13401

[24] A. Shaller, L. Zamir, M. Nojoumian, "Roadmap of Post-Quantum Cryptography Standardization: Side-Channel Attacks and Countermeasures", *Information and Computation*, vol.295, 2023, pp.105-112, https://doi.org/10.1016/j.ic.2023.105112

[25] Cao Yuanlong, Li Junjie, Chakraborty Chinmay, Qin Le, "Temporal Segment Neural Networks-Enabled Dynamic Hand-Gesture Recognition for Industrial Cyber-Physical Authentication Systems", *IEEE Systems Journal*, vol.99, 2023, pp.1-12, https://doi.org/10.1109/ JSYST.2023.3306380

[26] R.I. Al-Khalid, R.A. Al-Dallah, A.M. Al-Anani, R.M. Barham and S.I.Hajir, "A Secure Visual Cryptography Scheme Using Private Key with Invariant Share Sizes", *Journal of Software Engineering and Applications*, vol.10, 2017, pp.1-10, http://dx.doi.org/10.4236/jsea.2017.101001

[27] X. Zhang, T. Gonnot and J. Saniie, "Real-Time Face Detection and Recognition in Complex Background" *Journal of Signal and Information Processing*, vol.8, 2017, pp.99-112, https://doi.org/10.4236/jsip.2017.82007