Hindawi
Mathematical Problems in Engineering
Volume 2020, Article ID 6287394, 9 pages
https://doi.org/10.1155/2020/6287394

Research Article

Reliability Evaluation of Public Security Face Recognition System Based on Continuous Bayesian Network

Zhiqiang Liu,[1,2,3] **Hongzhou Zhang**,[1] **Shengjin Wang**,[3] **Weijun Hong**,[1] **Jianhui Ma**,[4] **and Yanfeng He**[5]

[1]*School of Information Technology and Cyber Security, People's Public Security University of China, Beijing 100038, China*
[2]*College of Computer Science and Technology (Software College), Henan Polytechnic University, Jiaozuo 454003, China*
[3]*Department of Electronic Engineering, Tsinghua University, Beijing 100084, China*
[4]*Bureau of Science and Technology Information, Ministry of Public Security of China, Beijing 100741, China*
[5]*Zhongdian Yunke Information Technology Company Limited, Zhengzhou 450000, China*

Correspondence should be addressed to Zhiqiang Liu; 2459830187@qq.com and Hongzhou Zhang; zhang_ppsuc@163.com

Received 21 September 2019; Revised 16 April 2020; Accepted 23 April 2020; Published 25 May 2020

Academic Editor: Dimitris Mourtzis

For the sake of measuring the reliability of actual face recognition system with continuous variables, after analyzing system structure, common failures, influencing factors of reliability, and maintenance data of a public security face recognition system in use, we propose a reliability evaluation model based on Continuous Bayesian Network. We design a Clique Tree Propagation algorithm to reason and solve the model, which is realized by R programs, and as a result, the reliability coefficient of the actual system is obtained. Subsequently, we verify the Continuous Bayesian Network by comparing its evaluation results with those of traditional Bayesian Network and Ground Truth. According to these evaluation results, we find out some weaknesses of the system and propose some optimization strategies by the way of finding the right remedies and filling in blanks. In this paper, we synthetically apply a variety of methods, such as qualitative analysis, quantitative analysis, theoretical analysis, and empirical analysis, to solve the unascertained causal reasoning problem. The evaluation method is reasonable and valid, the results are consistent with realities and objective, and the proposed strategies are very operable and targeted. This work is of theoretical significance to research on reliability theory. It is also of practical significance to the improvement of the system's reliability and the ability of public order maintenance.

1. Introduction

The public security face recognition system belongs to the intelligent video surveillance system, which can identify face images automatically in policing video surveillance. As for public order maintenance in public areas, it is a type of special technical equipment, which is deployed, managed, and utilized by public security agency. The emergence of the system has epochal significance, which is another major sign of the development of the security technology. In recent years, public security agency is devoted to constructing a three-dimensional system for public order maintenance, which can combat, prevent, and control crimes. The system has been "quietly" applied, and it has become a significant part of the security system. However, the system is deployed in unconstrained real scene, which is especially vulnerable to the influence of illumination, posture, expression, occlusion, age, and other unpredictable interference factors. The reliability is quite limited [1]. As the system grows more complex, the reliability problem is becoming increasingly prominent, and it is getting a lot of attention from scholars and public security agency. The reliability has become a significant factor in system effectiveness. As an essential link of system effectiveness evaluation, reliability evaluation naturally becomes a crucial research topic of actual face recognition system.

Today, the research achievements about system reliability evaluation are few. There is no public report in the academic community. However, the research on reliability analysis of other complex systems is in the ascendant, which has become a hot spot in the research field of system

engineering [2]. Many mature theoretical achievements have been accumulated. The academic research on reliability begins in World War II, when the reliability analysis evolves from electronic system and aerospace system little by little [3]. Now, it has expanded into many fields, such as communication and machinery. Common reliability analysis methods are as follows: Fault Tree Analysis, Dynamic Fault Tree, Monte Carlo Simulation, Markov Process, Fuzzy Numbers, Failure Mode Effects and Criticality Analysis, Universal Generating Function, GO Methodology, Petri Net, Reliability Block Diagram, and Binary Decision Diagrams [4]. These methods have achieved some results for the reliability analysis of systems that match corresponding conditions, but they all have harsh application conditions and demands, and the modeling or calculating process is relatively complicated. In addition, some methods are not accurate enough. Consequently, the development and the application of these methods are more or less limited.

Although the academic community has not yet developed a specific reliability analysis method for the public security face recognition system, there have been some reliability analysis methods in the security system. Lv [5] evaluates the security equipment's reliability through fitting failure function and testing life. This method is rather complicated and time-consuming, and it only takes internal factors into account. Qu et al. [6] propose a risk evaluation indicator system and a Fuzzy Analytic Hierarchy Process model for a video surveillance system to evaluate its failure possibility, which amounts to reliability evaluation. The evaluation model is quite subjective, and most of the evaluation indicators are qualitative. Therefore, the selection of evaluation methods is the key to evaluating a system's reliability.

In order to find the weak links that affect the system reliability and put forward some system optimization strategies, we intend to construct a comparatively objective and valid reliability evaluation method for the public security face recognition system. We make a pioneering and beneficial attempt.This work may make more or less contributions to the development of the theory and technology of reliability analysis, it may make more or less contributions to filling the theoretical gap for reliability and effectiveness analysis of the public security face recognition system, and it may attract more valuable research. Accordingly, this work has theoretical significance. Furthermore, the measurement results and optimization strategies can make public security agency grasp the actual system's state clearly and improve its effectiveness and reliability. The study has practical significance.

2. Basic Work

The reliability requirements of the public security face recognition system are derived from public security business's demands for system functions. Therefore, the basic task of the system reliability analysis is to analyze public security business's demands for system functions. The analysis of the system reliability should start from analyzing functions.

2.1. Analysis of System Functions. The public security face recognition system is a combination of video surveillance technology combining with face recognition technology, which is also a booster for value and efficiency of the public security video surveillance. The main principle is to match target faces with real-time faces acquired by public security video surveillance cameras automatically with image matching technology. Today, the public security face recognition system has been a kind of crucially technical equipment for public security agency [7], and it will play an increasingly important part in public order maintenance.

Public security business's demands for system functions generally include the following three aspects: (1) Prevention, that is, effective prevention or warning before an event. The system can play a psychological deterrent and warning role for potential criminals, preventing their criminal acts in the bud. It can also monitor the whereabouts of some key populations closely. (2) Management and control, that is to manage and control criminals timely during an event. The traditional criminal management and control mainly relies on human watch and comparison. It is a time-consuming and labor-intensive task, and it is prone to cause false positive and false negative. The system can acquire real-time face images from the video surveillance front ends. It can automatically compare these real-time face images with those of watch list to realize automatically real-time control, watching target faces in important public places at all times; once the target faces appear in these places, control terminals will automatically alarm to prompt human intervention immediately. (3) Combating, namely, the efficient technical warfare method of cracking down on criminals after an event, including video image detection and forensics. Traditional video image detection and forensics can only rely on human access, viewing, and comparison. It is heavy workload, slow, and inefficient. Furthermore, police officers are prone to visual fatigue. The system can intelligently check the identity information of criminal suspects. It can discover case clues in massive historical video images to realize deep analysis for valuable information and then find the criminal clues and evidence of suspects quickly in historical video images.

Only when a public security face recognition system has higher reliability, it can meet the above-mentioned functional demands and thus can bring about a great improvement of the effectiveness of public order maintenance. Therefore, public security business's demands for system functions put higher requirements on the reliability. The ideal state of system operating is that the main components or links of the system can run without breakdown in all 7×24 hours, and its recognition error rate is as low as possible. The actual state is that any component or link has the possibility of failure, and the recognition error rate is not satisfactory. Any failure or error can result in the failure of the whole system. The purpose of the evaluation is to quantify and grasp the failure possibility and minimize it.

2.2. Analysis of System Structure, Common Failures, and Influencing Factors of the Reliability. The public security face recognition system is similar to other face recognition

systems in structure. It consists of six modules, which are acquisition subsystem, transmission subsystem, storage subsystem, identification subsystem, display subsystem, and control subsystem. The camera is a core device of the acquisition subsystem, which can acquire video images and convert them into transmittable signals. In addition, the acquisition subsystem also includes light supplement lamp, power supply, surge protective device, and mounting bracket. Common failures of the acquisition subsystem are power outage, camera malfunction, light supplement lamp breakdown, lens occlusion or deviation, etc. The transmission subsystem can transmit video image data and control signals. The transmission subsystem can be divided into two categories by the type of the signals, which are digital and analog. Currently, most transmission subsystems are digital. This paper only studies the digital system. The transmission subsystem mainly includes twisted pair or fiber, switch, and the like. Common failures of the transmission subsystem are power outage, line breakdown, electromagnetic interference, etc. The storage subsystem can store and access original video images, face models, and recognition results, whose primary task is to ensure the integrity and security of the data on the premise of ensuring the access quality. The public security face recognition system varies in storage modes depending on solutions. Most of the current systems apply the network video recorder (NVR) mode, and some of them apply the distributed storage or cloud storage mode. The storage subsystem includes storage device hardware and supporting software. Common failures of the storage subsystem are power outage, storage hardware malfunction, and software malfunction. The identification subsystem can mainly implement modeling of face features and compare models of acquired faces with those in the watch list in real time. If the similarity reaches a set threshold, the system will automatically warn. The identification subsystem includes identification device hardware and supporting software. Common failures of the identification subsystem are power outage, identification hardware malfunction, and software malfunction. The display subsystem can mainly display real-time or historical surveillance video images, operation state of the devices, recognition results, and alarm signals. The display subsystem includes display device hardware and supporting software. Common failures of the display subsystem are power outage, display hardware malfunction, and software malfunction. The control subsystem can mainly implement equipment management, authority management, scheduling code stream, switching video signal, controlling transmission, controlling network, controlling storage, and sending various application instructions. It is a core part of a public security face recognition system. The control subsystem includes control device hardware and supporting software. Common failures of the control subsystem are power outage, control hardware malfunction, and software malfunction. According to the above analysis, we can get eighteen narrow-sense influencing factors of the reliability. Due to the system's particularity, there is a broad-sense influencing factor of the reliability that does not belong to failures, which is recognition performance. So, there are nineteen influencing factors of the reliability in total.

3. Method

The reliability of the public security face recognition system refers to the possibility that it remains in an effective or normal working state. It reflects the continuous stability that the system provides technical support to public security business. The reliability reflects a system's running state from a quantitative perspective. Reliability evaluation is mainly to measure the possibility that the system reaches an expected state [8]. It is an unascertained causal reasoning problem. There may be some incomplete information. There are both binary and polymorphic modules, both parallel and serial modules, both independent and related modules, as well as both redundant and nonredundant modules in the system. The structure is rather complex, and the types are various. Therefore, in the light of these characteristics, an advanced and valid model should be developed to measure the system's reliability scientifically and reasonably.

3.1. Continuous Bayesian Network. Bayesian Network is also referred to as Belief Network, which is one of the most effective theoretical models in unascertained knowledge description and reasoning. It is also one of the main and the most widely used methods of system reliability analysis [9]. It is a directed graphical description based on network structure, and it is a combination of artificial intelligence, probability theory, graph theory, and decision theory. It has become a mainstream method and research hot spot in the fields of artificial intelligence and unascertained knowledge representation and reasoning.

Bayesian Network modeling is based on a directed acyclic graph. It is a mathematical method of probabilistic reasoning, which is defined completely [10]. It expresses information elements with node variables, and it expresses the relationship between information elements with a directed edge. However, the traditional Bayesian Network can only express discrete variables. Our proposed model is called Continuous Bayesian Network, which has distinct advantages in infinite states and logic descriptions of nondeterministic failures [11]. Its advantages are as follows: (1) the Continuous Bayesian Network is a visualized model of representing unascertained causal relationship, whose ability to process unascertained information is very high; (2) the Continuous Bayesian Network can describe continuous variables; (3) the Continuous Bayesian Network can fuse multi-source information effectively; (4) the Continuous Bayesian Network modeling is simple, while reasoning objectively. Because of these advantages, this paper constructs a Continuous Bayesian Network model to measure the reliability of the public security face recognition system.

3.2. Basic Data for Evaluation. The raw data are derived from operation and maintenance records of an actual face recognition system of a public security bureau within 2 years. The system passed the acceptance test in March 2017, and it was officially put into use in April of the same year. The system has 60 high-definition cameras for face recognition, whose installation locations are distributed in large-scale

markets, shopping malls, bus stations, overpasses, and other crowded places. In this paper, after counting and processing the maintenance data, we acquire some related information, such as failure time, position, module, cause, the number of image channels affected, and duration of failure. Partially statistical results are shown in Table 1. There are more than 100 times failure events in total, which, respectively, occur in the acquisition subsystem, transmission subsystem, storage subsystem, identification subsystem, display subsystem, and control subsystem, including power-off events of each subsystem. Modeling and reasoning of the Continuous Bayesian Network are based on the basic data.

3.3. Modeling. The primary task of modeling the Continuous Bayesian Network is to determine the network nodes. As for the reliability evaluation model, it is to serve the nineteen specific influencing factors as root nodes, six subsystems as internal nodes, and system reliability as a leaf node. We first form an adjacency matrix according to the relationship between influencing factors of the reliability, subsystems, and system reliability. The model framework of the Continuous Bayesian Network can be acquired through connecting relevant nodes with directed edges according to the adjacency matrix. We draw the model framework by programming in R language. The model framework is shown in Figure 1. The conditional probabilities between nodes can be determined in accordance with equation $P(T = 1 \mid \exists r_i = 1) = 1$ and equation $P(T = 1 \mid \forall r_i = 0) = 0$, where P represents a conditional probability between parent node r_i and child node T, 1 represents failure, and 0 represents no failure. When the influencing factors are narrow-sense ones, several related reliability parameters of the corresponding root nodes can be calculated or measured as follows, including failure rate, failure restoration time, cumulative time of failure restoration, and failure possibility.

(1) Failure rate

The failure rate refers to failure times of an influencing factor within a quarter, in unit of times. In order to analyze and calculate conveniently, the failure rate of each influencing factor is uniformly converted into the number of corresponding image channels affected, which is called equivalent failure rate.

(2) Failure restoration time

The failure restoration time refers to the duration from the occurrence of a failure to complete restoration, namely, the invalid duration of a factor, usually in unit of minute.

(3) Cumulative time of failure restoration

The cumulative time of failure restoration refers to the sum of the restoration time of a factor within a quarter, that is, the total failure time of the factor within a quarter, in unit of minute. In order to analyze and calculate conveniently, the cumulative time of failure restoration of each factor is uniformly converted into the cumulative failure time of corresponding image channels affected. Suppose that λ_j is failure rate of factor X_i in the j^{th} quarter, T_{jk}^R is the failure restoration time of the k^{th} failure in the j^{th} quarter, and n_{jk} is equivalent failure rate of the k^{th} failure in the j^{th} quarter. The computation equation of the cumulative time of failure restoration of X_i in the j^{th} quarter is given by

$$T_{ij}^{AR} = \sum_{k=1}^{\lambda_j} n_{jk} T_{jk}^R. \tag{1}$$

(4) Failure coefficient and failure possibility

The failure coefficient refers to the proportion of a factor's failure time in a whole quarter. According to the basic data, we can obtain failure coefficient and related parameters of each factor in each quarter. The statistical results of a quarter are shown in Table 2. The failure possibility refers to the average of failure coefficients of each factor within 2 years. It is also an estimated value of a factor's failure probability in the case of considering failure rate and maintenance efficiency. Under the condition where failure time obeys exponential distribution, the failure possibility of factor X_i is given by

$$\prod_i = E(\Upsilon_i) = \frac{1}{q} \sum_{j=1}^{q} \Upsilon_{ij}, \tag{2}$$

where Υ_{ij} is the observation value of the failure coefficient of factor X_i in the j^{th} quarter. q is the total observation times. Υ_{ij} can be calculated according to the following equation:

$$\Upsilon_{ij} = \frac{T_{ij}^{\text{AR}}}{90 \times 24 \times 60 \times N}, \quad (i = 8, 9, \ldots, 19, 21, \ldots, 26), \tag{3}$$

where 90 is the number of days in a quarter, 24 is the number of hours in a day, and 60 is the number of minutes in an hour, and N is the total of face cameras of the system.

When the influencing factor is the broad-sense one, specifically recognition performance, the recognition error rate is used as the failure coefficient. We evaluate false-negative identification rate (FNIR) for the system on face recognition dataset of LFW BLUFR when false-positive identification rate (FPIR) equals to 1%. At this point,

$$\Upsilon_{ij} = \text{FNIR}_{ij} = \frac{\text{FN}_j}{\text{TP}_j + \text{FN}_j}, \quad (i = 20). \tag{4}$$

For FNIR_{ij}, TP_j denotes the number of samples that are predicted to be positive ones which are actually positive in the j^{th} quarter and FN_j denotes the number of samples that are predicted to be negative ones which are actually positive in the same quarter. We put the computation result of equation (4) into equation (2) to get failure possibility of this factor.

Geer and Klir [12] propose "Information preserving transformation" in the process of transformation between probability and possibility, that is, the uncertainty in information remains unchanged in the process of mutual transformation between two theories. Their proposed conversion equations are as follows:

Table 1: Basic data statistics (partial).

Failure time	Failure position	Failure module	Failure cause	The number of image channels affected	Duration of failure (minutes)
May 11, 2017	Northeast entrance to a certain market	Acquisition subsystem	Regional outage	1	62
May 11, 2017	Overpass of a certain road	Acquisition subsystem	Regional outage	1	62
May 11, 2017	East entrance to a certain mall	Acquisition subsystem	Regional outage	1	62
May 11, 2017	South entrance to a certain mall	Acquisition subsystem	Regional outage	1	62
May 11, 2017	North entrance to a certain mall	Acquisition subsystem	Regional outage	1	62
May 20, 2017	A certain bus stop	Acquisition subsystem	Lens occlusion	1	106
July 15, 2017	Bus station	Acquisition subsystem	Camera malfunction	1	213
July 22, 2017	Command center of the public security bureau	Transmission subsystem	Server room outage	60	33
July 22, 2017	Command center of the public security bureau	Storage subsystem	Server room outage	60	33
July 11, 2017	Command center of the public security bureau	Identification subsystem	Server room outage	60	33
July 11, 2017	Command center of the public security bureau	Control subsystem	Regional outage	24	63
July 11, 2017	Command center of the public security bureau	Display subsystem	Regional outage	24	63
August 17, 2017	Command center of the public security bureau	Transmission subsystem	Server room outage	60	15

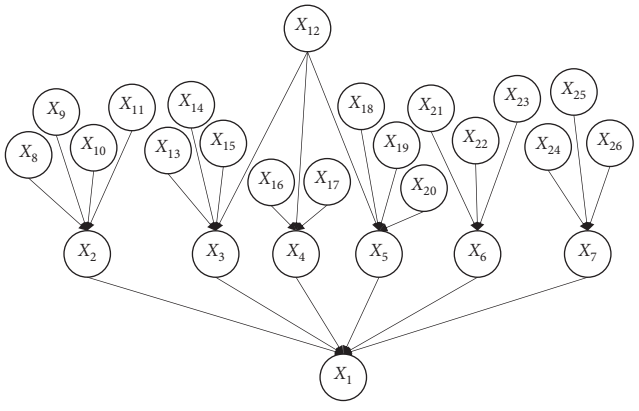

Figure 1: Continuous Bayesian Network model.

$$P_i(E=1) = \frac{\Pi_i^{1/\alpha}}{(1-\Pi_i)^{1/\alpha} + \Pi_i^{1/\alpha}}, \tag{5}$$

$$P_i(E=0) = \frac{(1-\Pi_i)^{1/\alpha}}{(1-\Pi_i)^{1/\alpha} + \Pi_i^{1/\alpha}}. \tag{6}$$

The prior probabilities of root nodes in the Continuous Bayesian Networks can be calculated through equations (5) and (6).

3.4. Reasoning. The most basic forms of Continuous Bayesian Network reasoning are causal reasoning and diagnostic reasoning. Causal reasoning is to infer a result by reasons. On the basis of the specific and known reasons—also called evidences, the occurring probability of the result under the reasons' conditions is calculated through reasoning. It is also called top-down reasoning. Diagnostic reasoning is to infer reasons by a result. On the basis of the specific and known result information, the reasons that cause the result and corresponding probabilities are obtained through reasoning. It is also called bottom-up reasoning.

We adopt causal reasoning that is to calculate the failure probability of each subsystem in accordance with the prior probabilities of specific influencing factors in the public security face recognition system and then calculate the reliability coefficient of the whole system.

Table 2: Failure coefficient and related parameters of each factor.

Influencing factors	Failure	Equivalent failure rate (times)	Cumulative time of failure restoration (minutes)	Failure coefficient
Power supply for front-end equipment	Outage	30	2176	0.000259
Camera	Malfunction	1	259	0.000031
Light supplement lamp	Breakdown	2	446	0.000053
Lens	Occlusion or deviation	1	565	0.000067
Power supply for server room	Outage	20	2176	0.000259
Power supply for transmission line	Outage	21	2587	0.000308
Line	Breakdown	2	553	0.000066
Electromagnetic environment	Interference	1	0	0
Hardware of storage	Malfunction	2	365	0.000043
Software of storage	Malfunction	20	2176	0.000259
Hardware of identification	Malfunction	20	2587	0.000308
Software of identification	Malfunction	30	4461	0.000530
Recognition performance	—	—	—	0.177101
Power supply for display	Outage	19	5650	0.000672
Hardware of display	Malfunction	0	0	0
Software of display	Malfunction	0	0	0
Power supply for control	Outage	25	2176	0.000259
Hardware of control	Malfunction	0	0	0
Software of control	Malfunction	0	0	0

Input: $\widetilde{G}$—A Continuous Bayesian Network; $\widetilde{\mathcal{T}}$—A Clique Tree that covers Continuous Bayesian Network $\widetilde{G}$; **E**—Evidence variable; **e**—Value of evidence variable; Q—A Query variable;
Output: $\widetilde{P}(Q|\mathbf{E})$—System reliability coefficient;
(1) Initialize $\widetilde{\mathcal{T}}$ with $\widetilde{G}$, that is, store probability distribution functions of $\widetilde{G}$ in each node of $\widetilde{\mathcal{T}}$;
(2) In the functions of $\widetilde{\mathcal{T}}$, assign value **e** to evidence variable **E**;
(3) Find a Clique C_Q containing Q in $\widetilde{\mathcal{T}}$, and regard it as a pivot;
(4) **for** (each Node C being adjacent to C_Q) **do**
(5) Call subroutine CollectMessage $(\widetilde{\mathcal{T}}, C_Q, C)$ to get a function;
(6) **end for**
(7) Multiply the function obtained in the previous step and the function stored in C_Q to obtain function $h(C_Q')$ of C_Q', where $C_Q' = C_Q \backslash \mathbf{E}$;
(8) **return** $\sum_{C_Q'} \backslash \{Q\} h(C_Q') / \sum_{C_Q'} h(C_Q')$.

Algorithm 1: Clique Tree Propagation $(\widetilde{\mathcal{T}}, \mathbf{E}, \mathbf{e})$.

Input: $\widetilde{\mathcal{T}}$—Initialized Clique Tree; C', C—Two adjacent nodes in $\widetilde{\mathcal{T}}$;
Output: f—A Function, i.e. information transmitted from C to C';
(1) Let $f_1, f_2, \ldots, f_l$ be functions stored in node C, and let $Y = C \backslash (C' \cup \mathbf{E})$;
(2) **if** (C is a leaf node of $\widetilde{\mathcal{T}}$) **then**
(3) **return** $\sum_Y \prod_{i=1}^{l} f_i$;
(4) **else**
(5) Let $C_1', C_2', \ldots, C_k'$ be nodes that are adjacent to C with the exception of C';
(6) **for** $(j = 1 \longrightarrow k)$ **do**
(7) $g_j \longleftarrow$ CollectMessage $(\widetilde{\mathcal{T}}, C, C_i')$;
(8) **end for**
(9) **return** $\sum_Y \prod_{i=1}^{l} f_i \prod_{j=1}^{k} g_j$;
(10) **end if**

Algorithm 2: CollectMessage $(\widetilde{\mathcal{T}}, C', C)$.

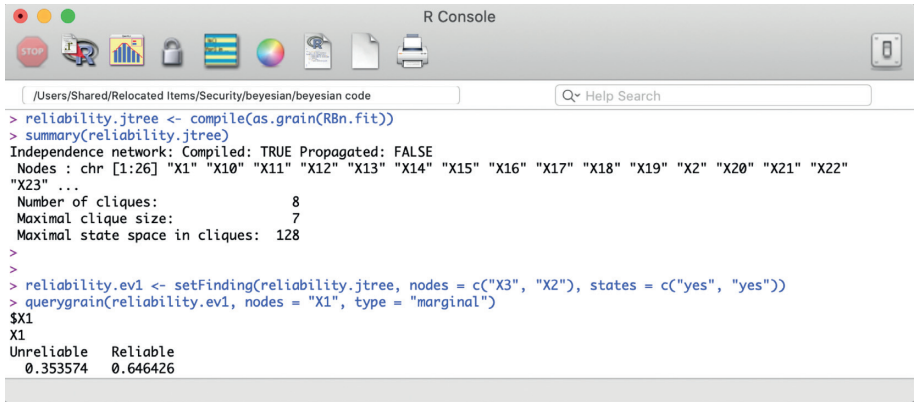

Figure 2: Reasoning results of the Continuous Bayesian Network.

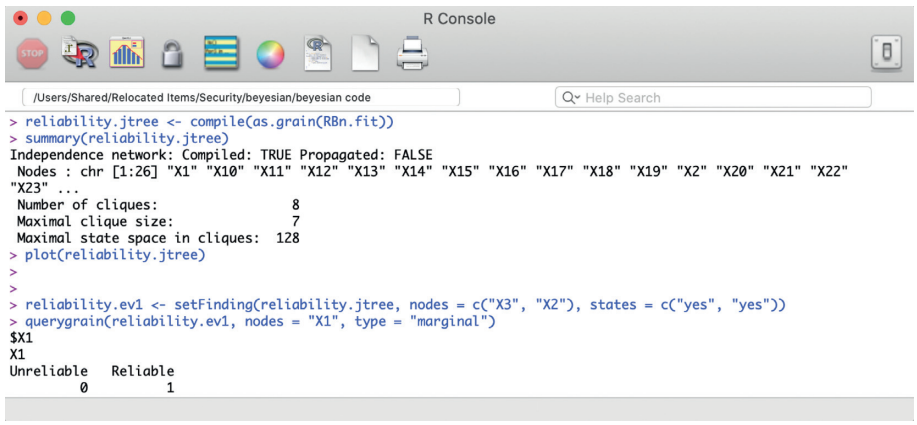

Figure 3: Reasoning results of the traditional Bayesian Network.

In practical applications, the structure of the Continuous Bayesian Network model is usually complicated, and the process of manual reasoning calculation is rather difficult. Therefore, automatic algorithms are needed for more efficient reasoning calculation. At present, the solution algorithms of the Continuous Bayesian Network can be divided into the exact reasoning algorithms and the approximate reasoning algorithms. The exact reasoning algorithms include Multitree Propagation, Clique Tree Propagation, and Combination Optimization. Among them, Clique Tree Propagation is most commonly used because of its accuracy, efficiency, simplicity, and applicability. The principle of the Clique Tree Propagation algorithm is to convert the Continuous Bayesian Network into another equivalent expression graph—Clique Tree, and then implement the probability reasoning and calculating through transmitting information on Clique Tree. The implementation process of the Clique Tree Propagation algorithm for single query variable is as follows (Algorithms 1 and 2).

Then, $P(Q|\mathbf{E} = \mathbf{e}) = \sum_{C_Q'} \setminus \{Q\} h(C_Q') / \sum_{C_Q'} h(C_Q')$ is just a query result, that is, system reliability coefficient.

We realize the calculation and reasoning process by programming in R Language. The system's state probabilities are acquired by running the programs. The results are shown in Figure 2. In the reasoning process, there are 8 cliques created in total. The maximal number of clique nodes is 7, and the maximal number of state spaces is 128. The reliability coefficient of the system is 0.646426.

4. Results and Discussion

The evaluation results show that the reliability coefficient of the public security face recognition system is 64.6426%. The system's reliability is not high enough. In this state, even if a watch target appears in the field of view of any camera, the possibility of system warning is 64.6426%. For public security agency, the system plays a considerably auxiliary role in the work of public order maintenance. As shown in achievement records of the system, more than 120 suspects are successfully matched and arrested with the face recognition technology within 2 years. Compared to traditional video detection means that rely on manual comparison, the system is highly efficient. Therefore, the system's reliability can meet the requirements of public order maintenance to a certain extent. However, the system has a failure probability of 35.3574%. Some cases may just happen in the period of system failure. On August 17, 2017, a robbery occurred at a certain bus stop, and the location of the crime is in the field of view of a face camera. However, the core switch in sever room was in power-off state. The face images of suspects were not recorded by the system but by a civil camera of a

Table 3: Comparison between the Continuous Bayesian Network and the traditional Bayesian Network.

Method	Reliability coefficient (%)	Ground Truth (%)	Inference error rate (%)
Continuous Bayesian Network	64.6426	64.1711	0.7348
Bayesian Network	100	64.1711	55.8334

nearby mall. Consequently, the police officers on duty nearby missed the opportunity to arrest. Obviously, the higher the system reliability, the less such kind of coincidences will be. Statistically, 67 suspects are arrested by the public security bureau through the traditional video surveillance system within 2 years. We serve these 67 suspects as slipping fish through the net of the face recognition system. We calculate recall rate, $\text{Recall} = \text{TP}'/(\text{TP}' + \text{FN}') = 120/(120 + 67) = 64.1711\%$, and serve it as the Ground Truth of the system reliability.

In order to verify the accuracy of the evaluation results of the Continuous Bayesian Network model, we also conduct an evaluation experiment on an existing method, traditional Bayesian Network. Firstly, we discretize the continuous node variables, then calculate the prior probabilities according to equations (7) and (8), and finally use the Clique Tree Propagation algorithm to carry out the reasoning solution. The evaluation and reasoning results of the traditional Bayesian Network model are shown in Figure 3:

$$P_i(E = 0) = \frac{q_0}{q}, \tag{7}$$

$$P_i(E = 1) = \frac{q - q_0}{q}, \tag{8}$$

where q is the total number of observations on the failure coefficient of influencing factor X_i and q_0 is the number of the factor's unreliable state.

The comparison between the Continuous Bayesian Network and the traditional Bayesian Network in evaluation results is shown in Table 3.

On the basis of the comparison, it is found that there is a large difference between the evaluation results of the traditional Bayesian Network and the Ground Truth in the system's reliability, while the difference between the Ground Truth and the evaluation results is severely closed with the Continuous Bayesian Network. The reliability coefficient gained from the Continuous Bayesian Network approximately equals to the Ground Truth. Thus, it is proved that the Continuous Bayesian Network has obvious advantages in describing continuous reliability variables.

The original intention and purpose of reliability evaluation is to find weak links of the system based on the evaluation results and then improve it. Statistically, the system's recognition performance has the greatest influence on its reliability, whose failure possibility accounts for 55.2757% of all the failure possibilities. For the system, first of all, its recognition performance should be improved. Specifically, optimize installation locations and parameters of face cameras, upgrade, and improve the face recognition algorithm timely. Secondly, the power of the system also has a great influence on its reliability, whose failure possibility accounts for 20.8468% of all the failure possibilities. The reliability of power supply for server room should be improved. Specifically, equip with generators for server room or increase capacity for unattended power source (UPS). Furthermore, the restoration time is a little long, resulting in a relatively high overall failure rate. There is still a large room for improvement in repair efficiency. It is necessary to improve maintenance efficiency and shorten restoration time. Specifically, send maintenance personnel that are experienced and professional rush to repair in the event of a major failure.

5. Conclusions

In this paper, we propose a new reliability evaluation method for the public security face recognition system, which is based on the Continuous Bayesian Network, and we design and realize the exact reasoning algorithm of the Continuous Bayesian Network—Clique Tree Propagation algorithm. Then, we solve and obtain the reliability coefficient of the system and compare the evaluation results of the Continuous Bayesian Network with those of traditional Bayesian Network and the Ground Truth of the system reliability. Finally, we propose some strategies for the improvement of the system's reliability in the light of the evaluation results. Because of the many advantages of the Continuous Bayesian Network, synthetic application of various methods, such as qualitative analysis, quantitative analysis, theoretical analysis, and empirical analysis, as well as the accuracy and validity of the basic data, the evaluation is quite objective and reasonable. The evaluation comparison experiments show that the reliability evaluation model based on the Continuous Bayesian Network is more scientific and reasonable, and the evaluation results are more consistent with realities and valid. So the reliability improvement strategies are comparatively targeted and operational too. The inadequacy of this paper is that the basic data for evaluation is small because it is relatively difficult to obtain data from the public security face recognition system, and the storage period of maintenance data is very limited. If maintenance data of more systems over a longer period of time can be acquired, the evaluation results will be more convincing and persuasive. Nevertheless, this paper pushes back the frontiers of the reliability analysis, opens up a new field for Bayesian Network modeling and reasoning, and proposes a novel model. The reliability evaluation results based on the proposed model can also be used for important parameters of system effectiveness evaluation. The proposed strategies can be used for some important decision references that help the public security bureau to improve the system's effectiveness and reliability. Accordingly, this paper has both theoretical and practical significance. In the future, we will attempt to

use the experience of the multiscale methods [13, 14] to measure the system's reliability.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

There are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported by the Basic Special Project of Ministry of Public Security of China (grant no. 2016GABJC01), the National Key R&D Program of China (grant no. 2016YFC0801003), and the Fundemental Research Funds of People's Public Security University of China (grant no. 2020JWCX14).

References

[1] Y. Tong, J. C. Zhang, and R. Chen, "Discriminative sparsity graph embedding for unconstrained face recognition," *Electronics*, vol. 8, pp. 1–21, 2019.

[2] E. Gascard and Z. Simeu-Abazi, "Quantitative analysis of Dynamic Fault trees by means of Monte Carlo simulations: event-driven simulation approach," *Reliability Engineering and System Safety*, vol. 180, pp. 487–504, 2018.

[3] J. Ai, W. Z. Su, and F. Wang, "Software reliability evaluation method based on a software network," in *Proceedings of the 29th IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW)*, S. Ghosh and R. Natella, Eds., Piscataway, NJ, USA, 2018.

[4] L. Meng, "Binary decision diagram model for reliability analysis of phased mission system," *Journal of National University of Defense Technology*, vol. 39, no. 3, pp. 184–192, 2017.

[5] H. T. Lv, *The research on key technologies of effectiveness evaluation for security system*, Ph.D Dissertation, 2014.

[6] N. Qu, H. J. Wang, and D. D. Wang, "Failure risk assessment of video surveillance system based on Fuzzy analytic Hierarchy process," *Journal of Shenyang University (Natural Science Edition)*, vol. 28, no. 2, pp. 128–131, 2016.

[7] Z. R. Zhang, "Talking about the construction and management of video surveillance system in public security," *China Public Security*, vol. 13, pp. 130–133, 2013.

[8] X. J. Li, *Urban traffic network analysis based on travel time reliability*, Ph.D Dissertation, 2015.

[9] D. Huang, C. Shan, M. Ardabilian, Y. Wang, and L. Chen, "Local binary patterns and its application to facial image analysis: a survey," *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 41, no. 6, pp. 765–781, 2011.

[10] M. Bereta, W. Pedrycz, and M. Reformat, "Local descriptors and similarity measures for frontal face recognition: a comparative analysis," *Journal of Visual Communication and Image Representation*, vol. 24, no. 8, pp. 1213–1231, 2013.

[11] C. Lu, T. Y. Zhang, W. Zhang, and G. Yang, "An experimental evaluation of linear and kernel-based classifiers for face recognition," in *Proceedings of the International Conference on Advances in Neural Networks–ISNN 2005 (LNCS 3497)*, J. Wang, X. Liao, and Z. Yi, Eds., Springer, Berlin, Germany, 2005.

[12] J. F. Geer and G. J. Klir, "A mathematical analysis of information-preserving transformations between probabilistic and possibilistic formulations of uncertainty," *International Journal of General Systems*, vol. 20, no. 2, pp. 143–176, 1992.

[13] Y. Dong, H. Wu, X. Li, C. Zhou, and Q. Wu, "Multiscale symmetric dense micro-block difference for texture classification," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 29, no. 12, pp. 3583–3594, 2019.

[14] Y. Dong, J. Feng, L. Liang, L. Zheng, and Q. Wu, "Multiscale sampling based texture image classification," *IEEE Signal Processing Letters*, vol. 24, no. 5, pp. 614–618, 2017.