EAI Endorsed Transactions
on Pervasive Health and Technology
Research Article EAI.EU

Remote medical video region tamper detection system based on Wireless Sensor Network

Sujuan Li[1], Shichen Huang[2,*1]

[1]College of Electronic Information Engineering, Hebi Polytechnic, Hebi 458030, China
[2]College of Information Science and Engineering, Hunan Normal University, Changsha 410081, China

Abstract

INTRODUCTION: A new telemedicine video tamper detection system based on wireless sensor network is proposed and designed in this paper.
OBJECTIVES: This work is proposed to improve the performance of telemedicine video communication and accurately detect the tamper area in telemedicine video.
METHODS: The sensor nodes in the sensing layer are responsible for collecting telemedicine video information and transmitting the information to the data layer. The data layer completes the storage of information and transmits it to the processing layer. The detection module of the processing layer detects the tampered area of the telemedicine video through two parts: suspicious moving point calculation and tamper detection, and transmits the detection results to the application display layer for display.
RESULTS: The experimental results show that the designed detection system can accurately detect the tampered area in the telemedicine video, and the packet loss rate is significantly reduced, and the maximum packet loss rate is no more than 1%.
CONCLUSION: The proposed detection system for remote medical video based on wireless sensor network can better meet the requirements of region tamper detection.

Keywords: Wireless sensor network; Telemedicine; Video area; Tampering detection system; Sensor nodes; Suspicious movement point

Received on 29 April 2022, accepted on 18 July 2022, published on 26 July 2022

doi: 10.4108/eetpht.v8i31.702

[1] Corresponding author. Email: hsc990423@hunnu.edu.cn

1. Introduction

From the current technical level, the level of medical information in our country is still in the stage of exploration and research. Especially in clinical nursing, most hospitals still use manual operation, which leads to the lack of accurate collection and classification of complex clinical nursing information and the poor effect of clinical nursing [1]. In order to relieve the pressure of medical staff and improve the medical level according to information technology, it is an urgent problem to be solved. Today, with the rapid development of wireless sensor networks, smart medicine has begun to enter people's vision and become an indispensable part of the development of medical information [2]. Smart medicine is to monitor and transmit the physiological parameter information of patients in real time through computer technology combined with wireless sensor networks, so as to quickly and accurately solve the problems of patients' medical needs. Telemedicine is an important part of smart medicine. Because some experts are far away from patients and it is difficult to reach them in a short time, it can be carried out through telemedicine or remote surgery. Therefore, a large amount of video resources need to be transmitted in the process of telemedicine. In order to create medical accidents or make patients panic, some illegal elements will tamper with the video resources of telemedicine, resulting in greatly reduced medical effects. Therefore, it is necessary to detect the tampering in the video area of telemedicine, which can avoid the above problems and improve the effect of telemedicine.

Wireless sensor network (WSN) is a multi hop self-organizing network system composed of a large number of cheap micro sensor nodes deployed in the monitoring area through wireless communication. Its purpose is to collaboratively sense, collect and process the information of the perceived objects in the network coverage area, and send it to the observer. The three elements of wireless sensor networks are sensors, observers and sensing objects [3]. Sensor nodes are composed of power supply, sensing unit, embedded processor, memory, communication unit and software. The observer is the user of the sensor network, the receiver and the applicator of the perceptual information. The observer can be a person, a computer or other device. The sensing object is the monitoring object of interest to the observer, which can be humidity, temperature, light, pressure, etc. Wireless sensor networks integrate the logical information world with the objective physical world, changing the interaction between human and nature [4]. People can directly perceive the objective world through sensor networks, thus greatly expanding the functions of existing networks and human ability to understand the world. Wireless sensor networks usually include sensor nodes, transmit nodes and sink nodes. A large number of sensor nodes are randomly deployed in or near the monitoring area. Under the guidance of the cluster head node, a routing topology is established. Then the sensor nodes collect and record the environment information of interest around [5], and transmit hop by hop along the previously established routing topology path. During the transmission process, the data may be processed by multiple forwarding nodes, and transmitted to the sink node after a single hop or multi hop routing [6], the sink node transmits the data to the gateway node through wired mode for centralized processing.

With the continuous development of Internet technology, illegal users can modify images or videos through image or video editing software, resulting in a serious reduction in the authenticity and effectiveness of image or video resources [7]. In order to ensure the authenticity of the original video content, academia has proposed many active forensics technologies, such as digital watermarking technology. The authenticity is verified by embedding authentication information when recording video, but active forensics technology requires embedding authentication information when recording video, which is difficult to achieve in real scenes. Therefore, passive forensics technology based on the characteristics of video itself has greater development and application space. Video’s inter-frame tampering detection technology is the main branch of passive forensics technology [8]. The main methods of video’s inter-frame tampering are: frame deletion, deleting one or part of the frames of the original video; Frame insertion, heterologous frame segments are inserted into the original video; Frame copy, homologous frame fragments are inserted into the original video. The existing inter-frame tampering detection methods are

mainly divided into two categories: methods based on the content discontinuity of tamper points and methods based on the periodic effect of secondary coding. There are too many images in the telemedicine video area, which is easy to be tampered with [9].

Lixiaohong and others proposed a mobile device image tamper detection method based on pruning compression CNN method [10]. Through the fusion of activation value and information entropy, the importance of CNN weighting can be effectively evaluated and the weighting with low importance can be cut off. Feedback adjustment is made according to the accuracy and pruning effect to control the balance of pruning compression. For pruning compression CNN, the corresponding convolution layer, pooling layer and adjustment layer are designed, which are analyzed and optimized from the perspective of layer and tampering mode respectively, and the tampering location is determined according to the correlation of image blocks. Gharbi et al. Used unsupervised Bayesian method to detect remote sensing images [11], accurately collected the information of video images through hierarchical Bayesian model and Gibbs sampler, and applied change detection based on Bernoulli model to remove the noise of the object to be detected, so as to ensure the operation efficiency of the algorithm. Yan Pu et al. Applied the multi support region local brightness order method to the forgery and tampering detection of video images [12], extracted the affine invariant region as the support region by using the maximum stable extreme region (mser) algorithm, and obtained multiple support regions with different scales, resolutions and directions by using the non sampling contourlet transform. The liop descriptors with rotation invariance and monotone luminance invariance are extracted from each support region, and the bidirectional distance ratio method is used to realize feature initial matching. Spatial clustering is used to classify the matched features, then random sampling consistency (RANSAC) algorithm is used to estimate the geometric transformation parameters of each classification, and necessary post-processing operations are used to detect the forged and tampered areas. The above three methods can achieve image tamper detection, but they have the defects of poor communication performance and can not be applied to remote medical video tamper detection. Therefore, the area tampering detection system of telemedicine video based on wireless sensor network is studied in this paper. The overall design scheme of the system is:

(1) The overall structure of the remote medical video region tamper detection system is designed. The system consists of five layers: perception layer, data layer, processing layer, network layer and application layer.

(2) The hardware of the system is designed according to the overall architecture of the system. The hardware includes wireless sensor network module and ZigBee chip. The wireless sensor network is used to collect the information of telemedicine video area, and ZigBee chip is responsible for the transmission of telemedicine video.

(3) According to the calculation results of suspicious moving points in the telemedicine video area, the suspicious video sequence of the telemedicine video is grayed, and the SIFT algorithm is used to extract the feature points of the frame, so as to complete the detection of tampered areas.

(4) Experimental verification, the tamper area location, energy suspicion and area tamper detection effect are taken as the system performance verification indicators for comparative verification.

2. Design of tamper detection system

2.1. Overall system structure

Telemedicine video's area tampering refers to that a key region of the video frame image is covered or replaced. After image editing and repair, the tampering trace is difficult to be distinguished by the naked eye. If the tampering operation is a malicious forgery, it will have a very serious impact and consequences. Therefore, the research on the detection and location of area tampering in telemedicine video has important research value and application prospect. According to the architecture of wireless sensor network technology, the area tampering detection system of telemedicine video is divided into five layers: perception layer, data layer, processing layer, network layer and application layer. The overall structure of the system is shown in Figure 1.

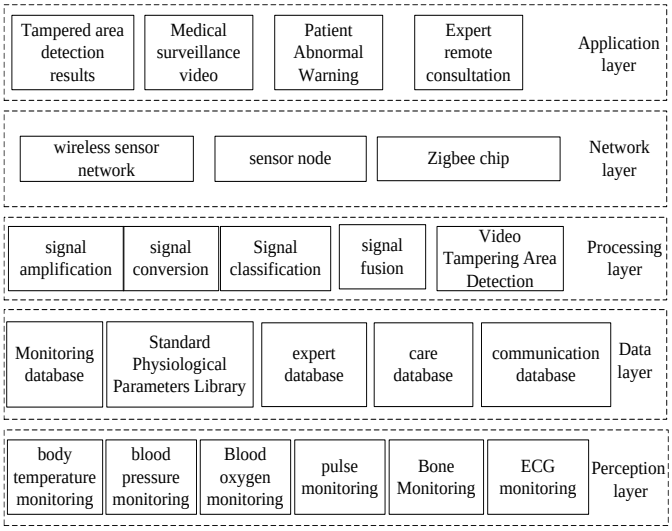


Figure 1. Overall structure of the system

The system uses the sensor of the sensing layer to collect the patient's body temperature, blood pressure, pulse and many other physiological parameters, and the collected data is transmitted to the data layer. The data layer stores the data and transmits the data to the processing layer at the same time. The video's area tampering detection module in the processing layer realizes the detection of tampering area in the telemedicine video through two parts: the calculation of suspicious moving points in the telemedicine video and the detection of tampering area in the telemedicine video. The area tampering detection results are transmitted to the application layer through the wireless sensor network of the network layer, and the application layer is used to display the tampering area detection results of telemedicine video.

The area tampering detection system of telemedicine video based on wireless sensor network mainly includes the following parts:

(1) Perception layer

In the designed system, the main function of the perception layer is to collect the physiological parameters of the corresponding parts of the patient, classify and aggregate the data information of different parts and upload it to the data layer. The data layer saves the data and transmits it to the processing layer at the same time. The system perception layer mainly realizes two functions: one is the collection of patient information, and the other is the classified transmission of different information. The patient information collected by the sensing layer includes identity recognition, body temperature collection, blood pressure collection, bone collection, ECG collection, pulse collection, etc. It mainly uses radio frequency identification technology, temperature sensor, bone mineral density sensor, pressure sensor, etc. to sense the corresponding human parts and obtain the corresponding electrical signals. While realizing the function, the system explores the best method of collecting information, and strives to achieve the accuracy of collecting information within ±0.01. Due to the need to collect physiological parameters of multiple parts of the human body, if each sensor is assigned a processor, it can not make full use of effective resources. The multi-channel transmission technology must be used to realize the separate transmission of different information, or the multi-sensor fusion technology must be used to realize the different classification of information. The system adopts wireless sensor network based on ZigBee specification. ZigBee specification analysis this system uses multiple sensors to measure multiple different parts of patients to build a large-scale wireless sensor network. Compared with other wireless transmission protocols [13], ZigBee specification has the application of wireless sensor networks that support star, tree and mesh network topologies, low power consumption, low cost and low data rate. In the specific development of the system, the beestack protocol stack of Freescale company is adopted, which uses direct sequence spread spectrum to divide the 2.4GHz frequency band into 16 non overlapping optional channels, so that the transmission of different channels will not interfere with each other. The disadvantage of ZigBee specification is that it adopts centralized management and requires gateway equipment.

(2) Data layer

The data layer includes five parts: monitoring database, standard physiological parameter database, expert database, nursing database and communication database. Each database in the data layer is used to store different types of data run by the system.

(3) Processing layer

The sensor device of the system transmits the collected data to the processing layer. The processing layer uses the video

tamper detection module to detect the tampered area of telemedicine video. The detection results of the tampered area of telemedicine video are transmitted to the application layer and returned to the database storage of the data layer. The sensor also needs to receive the control of the processing layer. The processing layer realizes this function through the controller. The system adopts the programmable system on chip PSoC of cypress micro systems in the United States. In addition to the microcontroller, PSoC also includes sufficient resources [14]. There is almost no need for external circuits for the development and design of the system. These resources can be combined freely, and their parameters can be selected or set. Coupled with the dynamic reconstruction function, they are enough to replace almost all common peripheral devices. The PSoC microcontroller used in the system enables developers to change from the original circuit chip design as the core mode to the combination mode of integrated system functions. It obviously reduces the volume of system products, shortens the development cycle, reduces the development cost and improves the development efficiency.

(4) Network layer

The network layer mainly transmits the processed patient data and the detection results of video tampering area to the server, realizes this function through the wireless transmission technology of GPRS module, and receives the control information sent by the host computer at the same time. Based on the transmission of a large number of patient data and information in the hospital, a server can be established in each nurse station to form a cloud computing platform with multiple massive data servers, and use cloud technology to store, analyze, mine and query data. Cloud computing platform is an important carrier for the development of hospital informatization. The use of computer distributed processing technology, grid computing and communication technology can solve the real-time and dynamic storage and calculation of massive data, realize the scientific rationality of data processing [15-16], query the diversity and load balance of server data sources, and promote the development of "intelligent medical treatment" and hospital service utilities.

(5) Application layer

The application layer of the system adopts B/S architecture, the processing layer uses C# language to transmit the processing information to SQL Server for storage through the network layer, and the application layer uses ASP Net language to realize the dynamic display of data. The client can log in to the system according to the corresponding permissions for access. The attending physician can view the human physiological parameters of the patient, set the treatment plan and write the doctor's order according to the patient's situation; The nurses in the nurse station can view the human physiological parameters of the patients in their departments, and care the patients according to the doctor's orders, human standard physiological parameters and intelligent expert tips; The patient's family members can check the patient's physiological parameters after logging in in different places according to the hospitalization number and the set password through intelligent devices, so as to understand the patient's condition in time and realize remote escort; At the same time, remote consultation of patients can also be realized by remote experts. The application layer displays the tamper detection results of telemedicine video to users through the display interface.

2.2. Design of system hardware

2.2.1. Wireless sensor network module

The master-slave node of wireless sensor network is responsible for the establishment and maintenance of wireless network, acquisition and transmission of various sensor data and other functions [17]. Therefore, it must have ZigBee communication module and sensor expansion interface. The hardware block diagram of the main nodes of the wireless sensor network module with CPU as the core is shown in Figure 2.

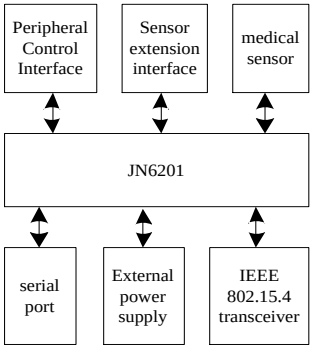


Figure 2. Wireless sensor network module

The IEEE802.15.4 transceiver in the node and the ZigBee protocol stack running on the CPU jointly realize the functions of wireless networking and data transmission. The node is powered by external power supply, and the node is powered by external battery. CPU and IEEE802.15.4 transceiver can choose JN6201 from Jennic, UK. This is a single-chip ZigBee baseband and RF module, which can easily realize the establishment and management of ZigBee wireless network and wireless data transmission. Since the built-in processor of JN6201 is a 32-bit RISC core with a speed of 16MHz, it can be used as the CPU of the node, which saves the cost of using an independent CPU and simplifies the hardware structure. The data transmission interface adopts the UART port of JN6201. The master node connects with the PC through this port, uploads data and receives instructions from the upper computer software. The slave node can connect with the RFID read-write module through this port as the interface for the RFID system to access the ZigBee network.

The onboard sensors on the slave node include general sensors and medical sensors, in which any digital sensor for testing vital signs can be selected as the medical sensor. We take the HKX-08A heart rate sensor module provided by Huake Electronic Research Institute as an example. It is a circuit module that integrates analog signal processing and digital processing technology to detect heart rate. The slave node can obtain its heart rate data through serial port.

In addition, in order to meet the processing needs of heart rate sensor, STC12C5A60S2AD microprocessor unit can be added. In this system, RFID is used to identify the identity of personnel to verify their legitimacy. RFID system includes reading and writing module and tag. The reading and writing module in this system adopts RMU900+ of Hengrui Electronics. This is an ultra miniaturized UHF RFID reading and writing module working in the 840-960MHz frequency band. It integrates PLL, wireless transmitter, wireless receiver, coupler, MCU components. It supports EPCC1GEN2/ISO18000-6C and ISO/IEC18000-6B protocols. It can connect with the slave node of the Internet of things through UART and upload tag ID and other information. The traditional card-type electronic tag can be selected as the personnel identity tag in this system.

2.2.2 ZigBee chip

ZIC2410 is the latest Zigbee/IEEE802.15.4 single chip microcomputer recently launched by AmericaCEL company. ZIC2410 includes an RF transceiver with baseband modem, hardwired MAC and a C8051F020 microcontroller. The device provides multiple general input / output pins, timers, UART and other peripheral functions, and provides a unique embedded voice codec, excellent data transmission rate (1M), excellent RF receiver and strong anti-interference technology. It is an ideal choice of ultra-low power consumption, plus 4 timers, voice circuits, 2 PWM and so on. In addition to excellent sending and receiving performance and selection performance, C8051F020MCU core supports low-power wireless communication function and ZigBee protocol stack.

ZIC2410 integrates link quality, high transmission rate, RF transceiver and voice codec, making it a truly unique 802.15.4/Zigbee single chip solution.

The main features of ZIC2410 are:

(i) The embedded 8051 microcontroller has 96KB embedded flash and 8kb data storage and programming space;
(ii) Data transmission rate: the rate of ZigBee is 300kbp / s, and the general application rate is 550kbp/s and 1mbp/s;
(iii) High wireless transmission sensitivity;
(iv) High wireless transmission power;
(v) Four power management modes. The current consumption in standby mode is less than 0.3uA, and external interruption can wake up the system;
(vi) Low voltage power supply is adopted (1.5V ~ 3.3V);
(vii) VOA and LNC are integrated on chip;
(viii) Four 8-bit ADC are integrated;
(ix) Integrated with IEEE802.15.4 standard transceiver;
(x) AES safety coprocessor is integrated;
(xi) It has the functions of battery detection and temperature sensing detection.

As a monolithic ZigBee chip with integrated CPU, ZIC2410 provides a high-performance and low-cost RF transceiver scheme for ZigBee network, which complies

with ZigBee specification and IEEE802 15.4 standard, and the highly intensive integration simplifies functional modules, reduces power consumption, and reduces the cost of the whole system to a new level. Zic2410 chip integrates 8051F020 microprocessor, which can realize data processing and control of external I/O port; It has 96KB FLASH, which can store data; It integrates temperature sensor, wireless transceiver module and so on.

2.3. Design of system software

The video's tampering area detection module realizes the detection of tampering area in telemedicine video through two parts: the calculation of suspicious moving points in telemedicine video and the detection of tampering area in telemedicine video.

2.3.1. Calculation of suspicious moving points in telemedicine video

At present, the frame-by-frame tampering repair technology to delete a target in the video is mainly to fill the deleted area through some repair algorithms. The frame sequence of video is continuous, and the repair operation is often difficult to ensure the continuity and consistency between the unmodified frame and the tampered frame, so that the tampered video leaves repair traces. These tampering operations usually use some fuzzy operations to embellish the modified area in order to cover up the tampered area, so as to change the energy proportion of the repaired area. Discrete cosine transform (DCT) is a spectrum analysis tool. Its transform core is cosine function. The basis vector of its transform matrix can well describe the relevant characteristics of speech signal and image signal. Therefore, in the transformation of speech signal and image signal, DCT transformation is considered to be a quasi optimal transformation.

The positive transformation formula of two-dimensional DCT is as follows:

$$F(u,v)=\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y)G(u)G(v)= \sqrt{\frac{2}{MN}}\cos\left[\frac{(2x+1)u\pi}{2M}\right]\cos\left[\frac{(2x+1)v\pi}{2N}\right] \quad (1)$$

In formula (1), M and N represent the length and width of telemedicine video image respectively. u and v represent image clockwise transformation and image counterclockwise transformation respectively.

The inverse transformation formula of two-dimensional DCT is as follows:

$$F(x,y)=\sum_{u=0}^{M-1}\sum_{v=0}^{N-1} f(u,v)G(u)G(v)= \sqrt{\frac{2}{MN}}\cos\left[\frac{(2x+1)u\pi}{2M}\right]\cos\left[\frac{(2x+1)v\pi}{2N}\right] \quad (2)$$

The definition of transformation coefficient $G(u)$ is as follows:

$$G(u)=\begin{cases}\frac{1}{\sqrt{2}} & u=0\\ 1 & other\end{cases} \quad (3)$$

$G(v)$ has the same definition as $G(u)$.

DCT transform has strong "Energy concentration" characteristics. The gray value distribution in the original image has a certain disorder, so it is difficult to observe any characteristics. After DCT transformation, the main energy of the image can be concentrated on a few low-frequency coefficients in the upper left corner, so that the energy decreases from the upper left corner to the lower right corner. The upper left corner is low-frequency energy, the lower right corner is high-frequency energy, and the middle is the transition from low-frequency to high-frequency. Generally, the low-frequency part reflects the area with slow gray change of the image, which is generally a flat area. The high-frequency part reflects the area with fast gray change of the image, such as edges and details. Low-high frequency energy ratio and frequency domain entropy are used to describe the proportion of low frequency energy and high frequency energy of an image.

The calculation formula of low and high frequency energy ratio of image is as follows:

$$B=\frac{1}{m\times n-r}\frac{(m\times n)\sqrt{\sum_{i=1}^{r}\beta_i^2}}{\left(\frac{1}{m\times n-r}\sqrt{\sum_{i=r+1}^{m\times n}\beta_i^2}\right)} \quad (4)$$

The calculation formula of frequency domain entropy of image is as follows:

$$H = -\sum_{i=1}^{m\times n}\left(\log_2 \frac{|\beta_i|}{\sum_{i=1}^{m\times n}|\beta_i|}\right)^2 \qquad (5)$$

Where, the image size is $m\times n$, and r represents the number of a few low-frequency coefficients concentrated in the upper left corner of the image after DCT transformation. The dimension of the two-dimensional array after DCT transformation is reduced by Z-scan from the upper left corner, so that the coefficients in the obtained one-dimensional array are sorted by decreasing energy, and β_i represents the i-th DCT coefficient after sorting. The numerator of B represents the mean value of image low-frequency coefficient, and the denominator represents the mean value of high-frequency coefficient. The larger the B is, the smaller the H is, indicating that the more the low-frequency components of the image are, the smoother the gray value distribution is; The smaller the value of B is, the larger the value of H is, which indicates that there are more high-frequency components such as edges and details of the image. In order to strengthen the change of image sequence energy value, according to the opposite characteristics of low-frequency energy ratio and frequency-domain entropy in energy proportion, the suspicious degree of image tampering energy is proposed to measure the suspicious degree of image tampering in telemedicine video. The calculation formula is as follows:

$$NT = \frac{1}{B} + 2H \qquad (6)$$

The suspicious degree of image tampering energy is to add the reciprocal of low-high frequency energy ratio to frequency domain entropy. The smaller the value of NT is, the more the low-frequency components and less high-frequency components of telemedicine video images are. If a target is removed from the image, some fuzzy retouching operations are usually used to mask the repaired area, which increases the low-frequency component of the image and reduces the energy suspicion. The telemedicine video is divided into image frame sequence, and the energy suspicious degree of each frame image is calculated. When there is no tampering, the energy suspicious degree between frames maintains continuity and consistency. If the moving target is removed from a certain frame sequence, the energy suspicious degree of each frame in the tampered sequence will be smaller than that of the non tampered frame, damaging the continuity and consistency between frames.

Assuming that there are n telemedicine video image sequences $f_1(x,y)$, $f_2(x,y)$, $f_3(x,y)$, ⋯, $f_n(x,y)$, usually $f_1(x,y)$ is the reference frame, and the initial value D_1 of the cumulative difference image and the initial value E_1 of the cumulative edge image are both 0, then the cumulative difference image D_k of frame k is calculated as follows:

$$D_k(x,y) = \begin{cases} D_{k-1}(x,y)+1 & |f_1(x,y) - f_k(x,y)| > T_1 \\ D_{k-1}(x,y) & other \end{cases} \qquad (7)$$

Where $1 < k \le n$. Each frame image of the image sequence of telemedicine video is compared with the reference frame image or the previous frame image. When the difference of the same pixel is greater than a certain threshold, the point corresponding to the pixel on the cumulative difference image will be increased by 1.

The cumulative edge image E_k of frame k is calculated as follows:

$$E_k(x,y) = \begin{cases} E_{k-1}(x,y)+1 & if\ f_k(x,y)\ is\ the\ edge\ point \\ E_{k-1}(x,y) & other \end{cases} \qquad (8)$$

Where $1 < k \le n$. For edge detection of each frame of telemedicine video image sequence, some classical edge detection operators can be used to extract image edge information, such as Canny operator, Roberts operator, Log operator and so on. If a pixel is the edge information of the image, the point corresponding to the pixel on the cumulative edge image is increased by 1.

The suspicious moving point image C_n is calculated as follows:

$$C_n(x,y) = \begin{cases} 0 & D_n(x,y) != 0 \,\&\, E_n(x,y) = 0 \\ D_n(x,y) & other \end{cases} \qquad (9)$$

For a pixel (x, y), when the gray value of the point changes greatly in the time domain and is not an edge information point, it is considered that the point may be tampered with, which is called a suspicious motion point, and the telemedicine video image sequence is a suspicious video sequence. According to the sequence results, the feature points of the frame can be extracted by SIFT algorithm to achieve regional tamper detection.

2.3.2 Detection of tampering in telemedicine video area

The suspicious sequence in the telemedicine video image sequence is detected through the above calculation, and the needs of the current frame are recorded to facilitate the subsequent region tampering detection. After graying the suspicious video sequence of telemedicine video, SIFT algorithm is used to extract the feature points of the frame $X = \{x_1, x_2, \cdots, x_n\}$. For each feature point, description operator $\{f_1, f_2, \cdots, f_m\}$ is included. Then the similarity of any two feature points is calculated to find the matching points. The Euclidean distance is used as the similarity measure. x_{ik} is noted as the k-th descriptor corresponding to the i-th feature point and x_{jk} is the k-th descriptor corresponding to the j-th feature point. Then the similarity calculation between the i-th feature point and the j-th feature point is expressed by the following formula:

$$T = \left[\sum_{k=1}^{m} \left(x_{ik} - x_{jk} \right)^2 \right]^{1/2} \quad (10)$$

According to formula (10), in the selection of threshold T, the larger the threshold is, the more matching feature points will be obtained, and the more mismatching points will be obtained; If the threshold is smaller, there are fewer false matching points, but there are fewer correct matching points. Through similarity calculation, the matching point set of the frame is obtained.

According to the characteristics of video area tampering, in order to ensure that the tampered content is meaningful and not easy to be found by the observer, the tampered video usually has three characteristics: (1) the tampered area is a connected area with a certain size; (2) The source region and the copy region have relatively concentrated similar feature points; (3) The tampered video frames are multiple (at least tens of frames) consecutive frames. According to the first feature of meaningful tampering of the above video, the number of matching point pairs is calculated. If the number of matching point pairs is less than 5, it is considered that the frame has not been tampered with, then the current = current +t frame is taken as the current frame for the next detection, and returned to the first part of the algorithm to continue detection; Otherwise, it is considered that the frame has been tampered with. At this time, it is necessary to determine the tampering area: according to the second feature of meaningful tampering of the above video, all feature points in the frame are divided into two categories according to their positions in the frame by using k-means clustering algorithm, namely source area and copy area; Then, circumscribed rectangles are made for the two types of areas respectively, the coordinates of the tampered area of the frame are recorded, and the tampered position is marked.

The detection process of tampering area in the telemedicine video area is shown in Figure 3.

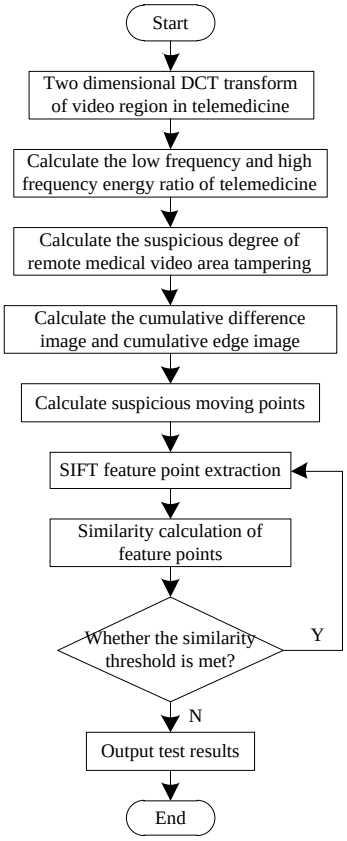
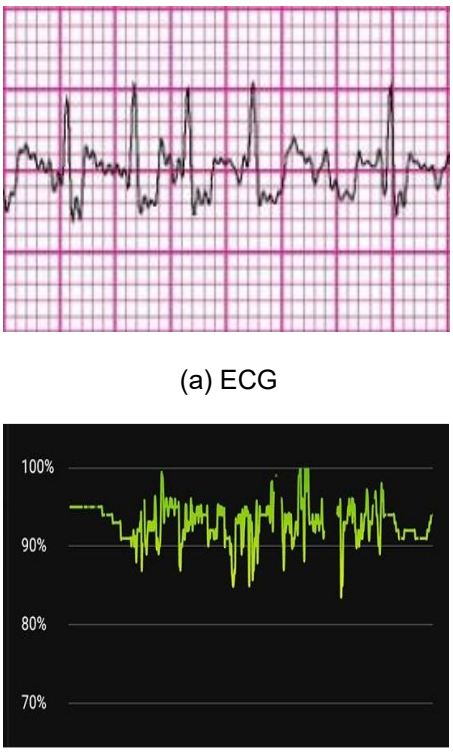


Figure 3. Remote medical video area tampering area detection process



(a) ECG

(b) blood sample saturation

Figure 4. Screenshot of the original monitoring video image of the telemedicine equipment

3. Results

In order to verify the effectiveness of the designed area tampering detection system of telemedicine video based on wireless sensor network for tamper detection in telemedicine video area, the proposed method is applied to the telemedicine equipment of a hospital. The hospital uses telemedicine equipment to monitor the real-time operation of patients, and the monitoring performance of telemedicine equipment is very important. Telemedicine equipment may be tampered, so it is very important to detect the tampering area of telemedicine video in time.

3.1 Experimental data

Collect the original monitoring information of telemedicine equipment as experimental data. The original monitoring image collected by telemedicine equipment in the hospital is shown in Figure 4.

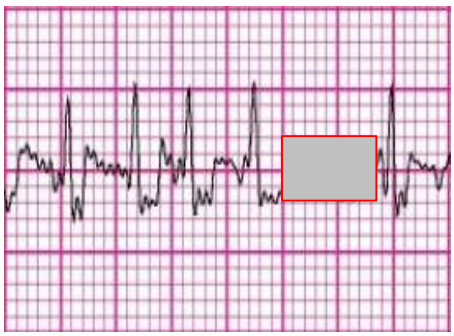
3.2 Experimental scheme and index

In order to fully verify the performance of the designed system, the tamper area location, energy suspicious degree and area tamper detection effect are taken as the indicators of system performance verification to verify the performance of the system in this paper. Taking the packet loss rate of the system operation as the comparison index, the system in this paper is compared with the pruning and compression CNN system proposed in reference [10] and the unsupervised Bayesian elimination proposed in reference [11].

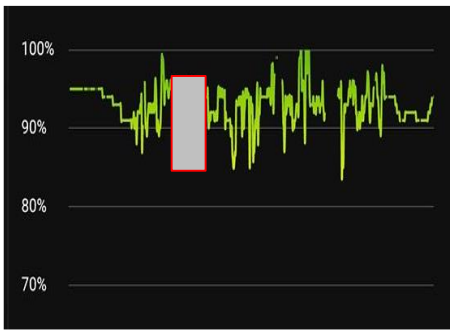
3.3 Analysis of experimental results

3.3.1 Tampering area positioning

The system designed in this paper is used to detect the regional tampering of telemedicine video, and the detection results are shown in Figure 5.



(a) ECG



(b) blood sample saturation

Figure 5. Tampering detection results of telemedicine video area

The red border gray area in Figure 5 is the tampering area of telemedicine video detected by the system in this paper. Through the comparison results of Figure 4 and Figure 5, it can be seen that the system in this paper can effectively detect the tampering area of telemedicine video. The area tampering detection results of telemedicine video is used to ensure the reliability of telemedicine video monitoring, and the accurate remote video monitoring results are used to improve the application effect of telemedicine video monitoring. This system can clearly detect the tampered area of telemedicine video, and can effectively locate the tampered area. When the tampering area is large, it still has effective detection effect.

3.3.2 Energy suspicion

The system in this paper is used to detect the tampered area of telemedicine video. Taking the telemedicine video monitoring results of blood oxygen saturation as an example, the energy suspicious degree in 1000 frames of telemedicine monitoring results is counted. The statistical results are shown in Figure 6.

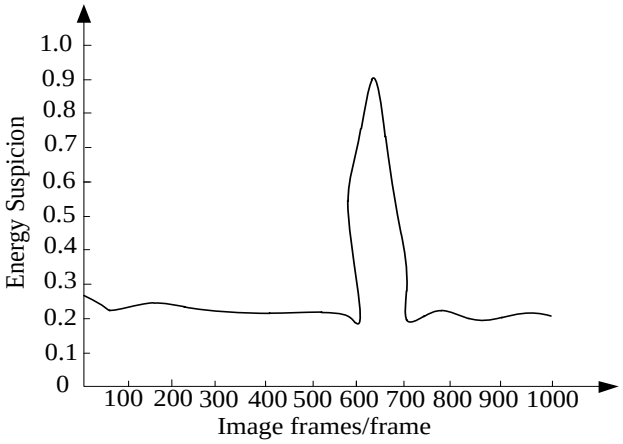


Figure 6. Energy Suspiciousness Curve

Through the experimental results in Figure 6, it can be seen that the system in this paper can effectively determine the energy suspicious degree of different frame images in the telemedicine monitoring video, and the telemedicine monitoring video frame with high energy suspicious degree has high possibility of tampering. The tampering area in the telemedicine monitoring video is obtained by calculating the energy suspicious degree calculation results of each frame of the telemedicine monitoring video. To further analyze the energy suspicious degree curve in Figure 6, when there is no possibility of tampering with the telemedicine monitoring video image, the energy suspicious degree difference between adjacent frames is small; When there is a possibility of tampering in the telemedicine monitoring video image, the image energy suspicion is significantly improved. Therefore, it can be seen that the energy suspicious degree can be used as an important basis to judge the tampered area of medical monitoring video.

3.3.3 Regional tamper detection effect

The system in this paper is used to detect the tampered area in the telemedicine monitoring video, and the detection results of the tampered area in the telemedicine monitoring video within 60min are counted. The statistical structure is shown in Table 1.

It can be seen from the experimental results in Table 1 that the system can effectively detect the tampering area of telemedicine monitoring video, and the accurate detection

of tampering area of telemedicine monitoring video can be used as an important basis to improve the monitoring performance of telemedicine monitoring equipment. Telemedicine monitoring video contains a large number of patients' physical health and personal privacy data. When there is tampering in the telemedicine monitoring video, the illegal physiological information enters the system, which affects the monitoring and diagnosis results of the telemedicine monitoring video, and the consequences are extremely serious. This system can effectively detect the tampering area of telemedicine monitoring video and improve the application performance of telemedicine monitoring video.

Table 1 The detection results of telemedicine monitoring video area tampering

Video serial number	total frames/frame	Tampered frames/frames	tampering with names
1	2584	152	remove tampering
2	3451	241	copy tampering
3	2846	163	Out-of-order tampering
4	3748	124	copy tampering
5	2985	185	copy tampering
6	3744	136	Out-of-order tampering
7	2845	124	copy tampering
8	2963	167	Out-of-order tampering
9	3974	185	remove tampering
10	2864	194	Out-of-order tampering

It can be seen from the experimental results in Table 1 that the system can effectively detect the tampering area of telemedicine monitoring video, and the accurate detection of tampering area of telemedicine monitoring video can be used as an important basis to improve the monitoring performance of telemedicine monitoring equipment. Telemedicine monitoring video contains a large number of patients' physical health and personal privacy data. When there is tampering in the telemedicine monitoring video, the illegal physiological information enters the system, which affects the monitoring and diagnosis results of the telemedicine monitoring video, and the consequences are extremely serious. This system can effectively detect the tampering area of telemedicine monitoring video and improve the application performance of telemedicine monitoring video.

3.3.4 Comparison test results of packet loss rate

The accurate physiological parameters collected by telemedicine monitoring video are an important basis for diagnosing the patient's physical condition. The accuracy of the collected physiological data is extremely important. The accurate physiological signal acquisition and transmission results can find the patient's condition in time. In this paper, the system uses sensors to collect the patient's physiological parameters, and transmits the collected patient's physiological parameters to the supervisor through wireless sensor network. The sensing performance of wireless sensor network is very important. Through the high transmission performance of wireless sensor network, it can ensure the transmission performance of telemedicine monitoring equipment and the detection performance of tamper detection system. The system in this paper is used to detect the tampering area of telemedicine monitoring video, the packet loss rate and transmission delay of transmitting different types of medical data. The system in this paper is compared with the system in reference [10] and the system in reference [11]. The statistical results are shown in Figure 7 and Figure 8.

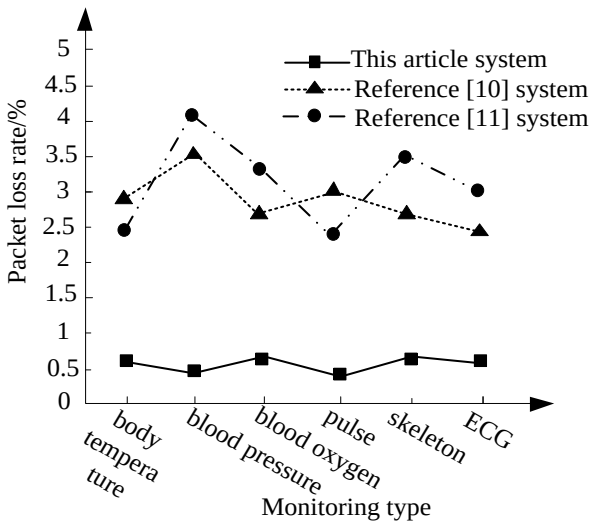


Figure 7. System running packet loss rate

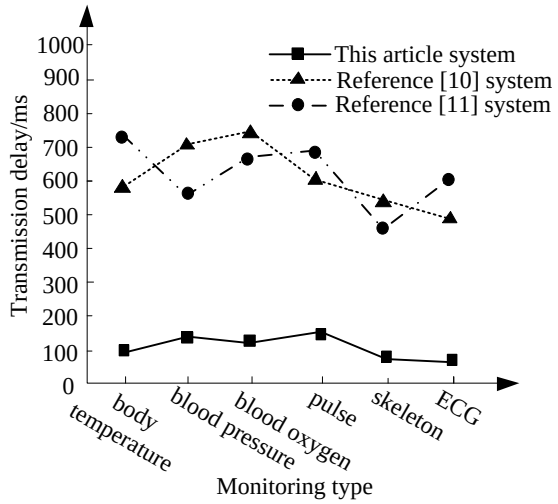


Figure 8. System operation transmission delay

As can be seen from the experimental results in Figure 7 and Figure 8, the system in this paper adopts wireless sensor network as the communication technology for tampering area detection of telemedicine monitoring video, and the communication performance is good. The packet loss rate of the system in this paper is significantly lower than that in reference [10] and reference [11]. In this paper, the system runs to detect the tampering areas of different types of telemedicine monitoring video images, and the packet loss rate is less than 1%; when the system in this paper runs to detect the tampering areas of different types of telemedicine monitoring video images, and the transmission delay is less than 200s. Figure 7 and Figure 8 verify that detecting the tampering area of telemedicine monitoring video image has high communication performance when the system is running.

4. Discussion

This paper studies the area tampering detection system of telemedicine video based on wireless sensor network, realizes telemedicine monitoring by using wireless sensor network, and detects the tamper in the video area of telemedicine monitoring. From the perspective of the network function of wireless sensor network, each forwarding node has the dual functions of information monitoring and routing. In addition to local information collection and data processing, it also needs to store, manage and integrate the data forwarded by other nodes, and cooperate with other nodes to complete some specific tasks.

At present, common wireless networks include mobile communication network, wireless LAN, Bluetooth network, ad hoc network, etc. Compared with these networks, wireless sensor networks have the following characteristics:

(1) Large scale network

In sensor networks, a large number of sensor nodes usually need to be deployed in the monitoring area, and the number of sensor nodes may reach thousands or even more. In addition, sensor networks can be distributed in a wide range of geographical areas, and the range of perception is also large. More comprehensive information can be obtained from different spatial perspectives. Through distributed processing of a large number of collected information, the accuracy of monitoring can be improved and the accuracy requirements of single node sensors can be reduced. The existence of a large number of redundant nodes also makes the system have strong fault-tolerant performance.

(2) Self-organization ability of network

Because in the monitored area, the sensors are randomly deployed in the area, the location of sensor nodes can not be accurately set in advance, and the mutual neighbor relationship between nodes is not known in advance. For example, a large number of sensor nodes are sown into the vast virgin forest by aircraft, or placed in inaccessible or dangerous areas at will. In this case, sensor nodes are required to have the ability of self-organization, and can be automatically configured and managed, to automatically form a multi hop wireless network system for forwarding monitoring data through topology control mechanism and network protocol.

In the use of wireless sensor networks, some sensor nodes fail due to energy depletion or other factors. In this case, the topology of the network is required to change dynamically. The self-organization of wireless sensor networks should be able to realize the dynamic change of network topology.

(3) Wireless sensor networks are data centric.

Any application system based on wireless sensor networks is inseparable from the management and processing technology of sensing data. In sensor networks, each sensor node has the functions of both end node and router. The sensor node receives the query or control command of sink. The core technologies are the technologies of data compression, data refining, data processing and data association based on sensor networks. Various implementation technologies of sensor networks must be integrated with these technologies.

5. Conclusion

In order to improve the security of remote medical video resources, a remote medical video region tamper detection system based on wireless sensor network is studied. The wireless sensor network is used as the communication technology of remote medical video region tamper detection to improve the application performance of remote medical video region tamper detection. Experiments show that the system can be applied to the actual remote medical video region tamper detection, and can effectively detect the tampered region in the remote medical video. It has high detection performance for deleting tampering, copying tampering and disordered tampering, and the packet loss rate of the system is significantly reduced. The packet loss rate of the system in this paper is less than 1%. Therefore, it fully shows that the proposed detection system based on wireless sensor network can better meet the requirements of remote medical video region tamper detection. However, the response performance of the system has not been verified in this study, so there is a problem of insufficient response performance. This problem will be studied in detail in subsequent studies.

Acknowledgement

The work was supported by Science and technology key topics of Hebi Polytechnic with No.: 2021-KJZD-004, Chinese University Industry-University-Research Innovation Fund- -Blue Point Distributed Intelligent Computing Project: Research on video tampering detection technology based on the joint characteristics of deep neural network and space-time.

References

[1] Liu X, Chen S, Song L, et al (2021). Self-attention Negative Feedback Network for Real-time Image Super-Resolution, Journal of King Saud University - Computer and Information Sciences, online first, 10.1016/j.jksuci.2021.07.014

[2] Liu S, Wang S, Liu X, et al (2022). Human Inertial Thinking Strategy: A Novel Fuzzy Reasoning Mechanism for IoT-Assisted Visual Monitoring, IEEE Internet of Things Journal, online first, 10.1109/JIOT.2022.3142115

[3] Vinodha, D. , Anita, E. M. & Geetha, D. M. (2021). A novel multi functional multi parameter concealed cluster based data aggregation scheme for wireless sensor networks (nmfmp-cda). Wireless Networks, 27(2), 1111-1128.

[4] Singh, P. & Mittal, N. (2021). An efficient localization approach to locate sensor nodes in 3d wireless sensor networks using adaptive flower pollination algorithm. Wireless Networks, 27(3), 1999-2014.

[5] Khalid H , Hashim S J , Ahmad S , Hashim F , Chaudhary M A . (2020). Cross-SN: A Lightweight Authentication Scheme for a Multi-Server Platform Using IoT-Based Wireless Medical Sensor Network. Electronics, 10(7):790-798.

[6] Gowda, C. S. & Jayasree, P. (2021). Rendezvous points based energy-aware routing using hybrid neural network for mobile sink in wireless sensor networks. Wireless Networks, 27(4), 2961-2976.

[7] Kim Tae Hyung, Park Cheol Woo, Eom Il Kyu. (2022). Frame Identification of Object-Based Video Tampering Using Symmetrically Overlapped Motion Residual[J]. Symmetry, 14(2):364-371.

[8] Ghamsarian, N. , Schoeffmann, K. & Khademi, M. (2021). Blind mv-based video steganalysis based on joint inter-frame and intra-frame statistics. Multimedia Tools and Applications, 80(6), 9137-9159.

[9] Liu S, Guo C, Fadi A, et al (2020). Reliability of Response Region: A Novel Mechanism in Visual Tracking by Edge Computing for IIoT Environments, Mechanical Systems and Signal Processing, 138, 106537

[10] Li, X. H. & Wang, X. X. (2021). An image Tamper Detection Method for CNN Mobile Devices Based on

Pruning Compression. Computer Simulation, 38(03), 83-86+91.

[11] Gharbi, W. , Chaari, L. & Benazza-Benyahia, A. (2021). Unsupervised bayesian change detection for remotely sensed images. Signal, Image and Video Processing, 15(1), 205-213.

[12] Yan Pu, Su Liangliang, Shaohui, Wu Dongsheng. (2019). Image forgery detection based on local intensity order and multi-support region. Journal of Computer Applications, 39(09):2707-2711.

[13] Liu S, Liu D, Gautam S, et al (2021). Overview and methods of correlation filter algorithms in object tracking. Complex & Intelligent Systems, 7: 1895-1917.

[14] Kociszewski R . Implementation of PI Controller in Reconfigurable PSoC Microcontroller to Control the Speed of Mobile Robot Drives[C]// 15th International Conference Mechatronic Systems and Materials (MSM2020). 2020.

[15] Narasimhamurthy S , Danilov N , Wu S , et al. (2019). SAGE: Percipient Storage for Exascale Data Centric Computing. Parallel Computing, 83(14):22-33.

[16] Li Shao, Huang Cheng. (2020). Simulation of Distributed Big Data Intelligent Storage Algorithm under Cloud Computing. Computer Simulation, 37(05):443-447.

[17] Singhal C , Patil V . (2021). HCR-WSN: Hybrid MIMO cognitive radio system for wireless sensor network. Computer Communications, 169(1):11-25.