Hindawi
Wireless Communications and Mobile Computing
Volume 2018, Article ID 5183451, 11 pages
https://doi.org/10.1155/2018/5183451

Research Article

The Improved Hill Encryption Algorithm towards the Unmanned Surface Vessel Video Monitoring System Based on Internet of Things Technology

Tingting Yang[1], **Yangyang Li**[1], **Chengzhe Lai**[2], **Jie Dong**[3] and **Minghua Xia**[4]

[1]*Navigation College, Dalian Maritime University, No. 1 Linghai Road, Dalian, Liaoning, China*
[2]*Telecommunication and Information Engineering College, Xi'an University of Posts and Telecommunications, Xi'an, Shaanxi, China*
[3]*Software College, Dalian University of Technology, China*
[4]*Electronics and Information Technology College, Sun Yat-Sen University, China*

Correspondence should be addressed to Tingting Yang; yangtingting820523@163.com

Received 19 June 2018; Accepted 10 September 2018; Published 3 October 2018

Guest Editor: Zhiqing Wei

Depending on the actual demand of maritime security, this paper analyzes the specific requirements of video encryption algorithm for maritime monitoring system. Based on the technology of Internet of things, the intelligent monitoring system of unmanned surface vessels (USV) is designed and realized, and the security technology and network technology of the Internet of things are adopted. The USV are utilized to monitor and collect information on the sea, which is critical to maritime security. Once the video data were captured by pirates and criminals during the transmission, the security of the sea will be affected awfully. The shortcomings of traditional algorithms are as follows: the encryption degree is not high, computing cost is expensive, and video data is intercepted and captured easily during the transmission process. In order to overcome the disadvantages, a novel encryption algorithm, i.e., the improved Hill encryption algorithm, is proposed to deal with the security problems of the unmanned video monitoring system in this paper. Specifically, the Hill algorithm of classical cryptography is transplanted into image encryption, using an invertible matrix as the key to realize the encryption of image matrix. The improved Hill encryption algorithm combines with the process of video compression and regulates the parameters of the encryption process according to the content of the video image and overcomes the disadvantages that exist in the traditional encryption algorithm and decreases the computation time of the inverse matrix so that the comprehensive performance of the algorithm is optimal with different image information. Experiments results validate the favorable performance of the proposed improved encryption algorithm.

1. Introduction

The Internet of things is widely used in intelligent transportation, environmental protection, government work, public safety, safe home, intelligent fire protection, industrial monitoring, environmental monitoring, street lighting control, landscape lighting control, building lighting control, square lighting control, square lighting control, elderly care, personal health, flower cultivation, water system monitoring, food traceability, enemy detection, and intelligence gathering. Based on the technology of Internet of things, the intelligent monitoring system of USV is designed and realized, and the security technology and network technology of the Internet of things are adopted. The intelligent perception of the self and environment information of the unmanned ship is realized by a variety of sensors. It is envisaged that developing an USV video monitoring system will greatly contribute to the maritime distress, urgency, safety, and general communications. The threat of maritime [1] piracy has mushroomed enormously in the past few years, especially in the detailed sea area below are piracy affected areas where the terror and threat of sea pirates have reached looming proportions: the strait of Malacca, the South China Sea, Gulf of Aden, and so on. The news channels on a daily basis have several incidents to report about pirates attacking crew and looting the vessel or hijacking a ship, and even causing

harm to the crew when their ransom demands are not met by the authorities. The maritime cloud server monitors the sea and collects a large amount of data [2–5] by USV video monitoring system; we will take timely and effective measures to deal with different situations by analyzing data. At the same time, it can collect information of a special area and obtain important information by this system, and experts can use these information to study whether the area can be expanded and whether there are available resources further. Video may be stolen and changed by pirates and other terrorists in the process of transmission that will pose a serious threat to information security of the sea; it is inconvenient to sea navigation, transportation, and any other activities of the sea. The encryption of video data has become priority, which is beneficial to the security of the sea and reducing losses and casualties.

With the development of information technology and the continuous progress of the society, there are more and more demands for information. Communication becomes convenient, quick and flexible by voice, data, image, and video in many ways at anytime and anywhere. In the past, the interaction of image and video information is a kind of extravagant demand for people, because of the limitation of network transmission technology and image compression ability. In recent years, with the increase of network bandwidth and the development of video image compression technology, people can carry out transmission of image and video through a variety of ways. In particular, with the progress of wireless transmission technology, the communication technology is affecting people's production and life in an unprecedented scale and degree [6]. The transmission of video and image information by wireless channels has become an urgent demand of application and the rapid improvement of network transmission technology; especially the wireless transmission technology could bring convenience to us, but it also brings hidden danger that sensitive image information may be stolen easily and spread illegally. Therefore, the security problem of image information has become a very important and crucial problem. Although the research of video encryption technology has been carried out for nearly 20 years, the existing secret strategy is not perfect and there is a large space for improvement, the encryption strategy of images transmitted under wireless conditions, whose degree of security is low. There are many different encryption methods and their respective systems have been formed but no performance of encryption strategy is satisfactory for all users. There are huge differences between various encryption strategies and the debates are hot. Video information security is an interdisciplinary subject spanning mathematics, cryptography, information theory, probability theory, computational complexity theory, and so on; it is related to video compression, network transmission, and application standards closely, which makes video encryption technology becomes a problem that has not been completely dealt with.

In this paper, a novel video encryption algorithm (i.e., Improved Hill encryption algorithm) is proposed, according to specific requirements of the wireless video monitoring system and combining with the research progress of video encryption technology. The algorithm combines with the process of video compression and regulates the parameters of the encryption process according to the content of the video image [4], so that the comprehensive performance of the algorithm is optimal for different image information. The results of the experiment are that the algorithm has good performance in the influence of adjacent pixels, and the information entropy of images is smaller than other algorithms. This work targets to investigate the security issues in maritime communication system, which is featured by protecting important data. Specifically, the contribution of this paper is threefold:

(1) We propose a novel video monitoring system of the USV to monitor the situation over sea, so that the authorities on the shore could obtain the video data in time and implement countermeasures for specific situations.

(2) A novel algorithm, namely, improved Hill encryption algorithm, is proposed, which has optimal comprehensive performance with respect to the security issue.

(3) It has been proved from the experimental results that the superior performance of the proposed improved Hill encryption algorithm.

The remainder of this paper is organized as follows. In Section 2, we discuss some related works. System model is presented in Section 3. The improved encryption algorithm is proposed, and the performance analysis is corroborated in Sections 4 and 5, respectively. In Section 6, we summarize the flow and indicate how the performance of the algorithm is improved.

2. Related Work

In recent years, driverless cars and UAV are becoming ever more popular among the public. Google Corporation is a pioneer in the field of research and development of driverless vehicles; the company announced that its unmanned vehicle project was developing to automated direction that is exclusion of human intervention at the end of May 2015 year. The prototype test of the automatic driverless vehicle will be carried out; it is expected that test of driving on the road can be carried out in a few years. At present, Google is making about 100 automatic vehicle models; UAV are striving to enter into people's lives, too. According to foreign media reports, online shopping giant Amazon is seeking permission from the US government to launch UAV flight test in the US. In fact, the research and exploration of USV are in progress in the field of unmanned technology, and ships floating on the sea will probably enter the unmanned era in the future. British Rolls Royce company (Luo Luo) is optimistic to this, as one of the [7] world's largest engine makers and shipbuilders who are determined to develop unmanned vehicles and offshore USV. There are slender difficulties in improving the unmanned craft at the technical level, and now there are many ships equipped with automatic equipment. The era of USV is seen in the future. Oscar Levand think that "In the near future, the USV will keep pace with the unmanned drones, the submarines and the unmanned vehicles that are being tested by Google". As far as water is concerned, the demand

of USV is strong. For example, while working on cruise and search, driverless technology can increase the number of ships that because it does not have to be manned and the size is small, its reaction is more responsive. To monitor the condition of the sea and collect important information by USV, once ships were attacked by pirate or the terrorist during the voyage, using video to capture the locations, numbers, features of the pirates, use of weapons equipment, and other important information, the information is transmitted to shore with unmanned vessel monitoring system. It should set a fixed time to transfer the collected information to the shore, it is convenience for shore personnel access to valid information in good time. Video should be sent to shore forcibly and take action in time in an emergency. The video data must be secure enough, once the data were intercepted and tampered that not only miss the best time to rescue and lose strong evidence.

In the multimedia computer technology application system, there are two research directions of video image processing. One is the compression encoding of the video image; the other is real-time processing of video image and protection of video information. In the video image compression algorithm, H.264 compression [8] algorithm as an international standard, because it has higher compression and it is able to provide a high quality image and supported by most of the operating platform, it also has good compatibility. H.264 has the following advantages: (1) coding efficiency: H.264 saves nearly 0.5 of its bandwidth compared with its predecessor H.263 and MPEG-4. (2) Superior quality images: H.264 can provide video images of high quality in low bit rate and image transmission of high quality on lower bandwidth is the highlight of H.264 application. (3) Improving network adaptability: H.264 can work in low delay mode under the real-time communication applications (such as video conferencing) and can also work in video storage or video streaming server that without delay. (4) Using hybrid coding structure: H.264 like previous H.261, H.263 use the hybrid coding structure, which is DCT transform coding and DPCM differential coding. At the same time, in order to improve the efficiency of compression coding, H.264 introduces a new coding methods under the structure of mixed coding, which adds new encoding methods, such as multimode motion estimation, intraprediction, and multiframe prediction, its content is based on variable length coding and 4x4 two-dimensional integer transform and improves the efficiency of coding. (5) H.264 has less coding options: a considerable number of options are often required to encode in H.263 that adds difficulty of coding, while H.264 achieves a concise "regression base" that reduces the complexity of the coding. (6) H.264 can be applied in different situations: H.264 can use different transmission and playback rates according to different environments and provide a rich tool of error handling that can control or eliminate the packet loss and bit error. (7) Error recovery function: H.264 provides a tool to solve the problem of network transmission packet loss, which is adapted for transmitting video data in a wireless network with transmission of high bit error rate. (8) Higher complexity: performance boost of H.264 is achieved at the expense of increasing complexity; it is estimated that the computational complexity of H.264 encoding is three times more than H.263 and the decoding complexity is twice as much as H.263.

The protection of video image information is to prevent sensitive information from being stolen and altered easily, copied, and disseminated illegally, including information encryption technology and information hiding. The encryption algorithm is built on the design of text data, the implementation of encryption that converts meaningful cleartext into meaningless ciphertext that is to prevent the information obtained during the process of data transmission by illegal interceptors. Video file has the characteristics of large data volume and require extraordinary real-time requirements, so it is difficult to gratify the requirements of video information on encryption efficiency that use traditional encryption algorithms sometimes. Spatial image encryption is encrypting the gray [9] scale of the image, because the gray scale (pixel value) of the image is the byte data that can be encrypted by means of data encryption. Therefore, the data encryption algorithm can be transplanted into gray scale encryption algorithm, which includes data encryption standard, simple Hill matrix encryption, and sequence encryption algorithm. In this paper a new image encryption algorithm is proposed that is based on the traditional Hill algorithm; we use an invertible matrix as a key to encrypt the image matrix and then transpose the encrypted image. Besides, the final step is double-layer encryption of matrix.

3. System Model

In this paper, we propose to use the LAN technology of Internet of things to construct the unmanned video monitoring system, the video node is connected with the different monitors of the USV through the local area network, and the control center can communicate with the maritime cloud service center that achieve the effect of information sharing. Compared with other methods, it has an advantage that it can be applied to USV of different sizes, so that we can design the USV video monitoring system according to the USVs size and structure, it just only to change the number of video monitoring nodes and location on the base of different requirements. The unmanned video monitoring system focuses on the security of ship navigation and cargo transportation. Monitoring the different locations over surface by configuring a certain number of cameras and other technological means, the information will be compressed and encrypted by SecurCore processor of DSP core and transmitted with three ways Figure 1. When the distance is far, the communication will be achieved by satellite and cloud platform and other shore-based or air-based facilities. We can select the corresponding schemes according to the distance, which saves the cost, decreases the time of communication, and avoids the waste of resources. The specific information transmission paradigms are shown in Figure 2.

3.1. Video Acquisition Module. The acquisition module of the video data is the input stage of information and its performance is very important to the whole system; the

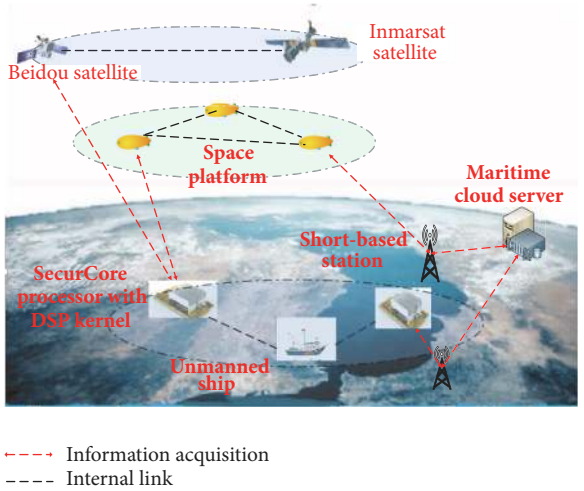

Figure 1: Information transmission diagram.

quality of the original video and image will determine the final image clarity of the maritime cloud server; the marine environment can be detected by sensors at sea, such as temperature sensors and thermosensitive components, light sensors and photosensitive elements, gas sensors and gas sensors, magnetic sensor, and subsensitive element. In this paper the module includes camera and corresponding control parts. The monitoring contents include the travel records of the ships and the meteorology of the sea as well as the transportation security of the goods and so on, it can also store and print pictures as the important evidence.

3.2. Video Compression and Encryption Module. The compression and encryption module of the video are the core of the unmanned video monitor system and its performance affects the overall performance of the system directly. The compression of video data is limited by various conditions, such as the transmission bandwidth, image resolution, frame rate, maximum delay of coding, and performance of processor. Therefore, the video compression module has to be coordinated with the transmission module, the encryption is integrated into the compression, and their relationship is very close. The module of compression and encryption can be implemented by SecurCore processor of DSP core.

3.3. Video Transmission Module. While the video data is completed by the hardware compression and it needs to be sent to the service platform through the network. However, there will be a few problems in the processing of sending, such as the simultaneous transmission of multiple monitoring nodes or the blockage of the network; it may occur that data is lose. In the process [10] of data transmission the network will judge the size of the packet, when the size is more than or less than the certain limit the packet will be discarded, the exact scope is (64-1500) bytes. RTP protocol is used to transmit video files because it is a real-time network transmission protocol that is often used for single point data transmission and it is very suitable for the transmission of audio and video data.

3.4. Video Playback Module. In the system, the shipboard service center needs to play video and image; according to their different purposes, the implementation is adopted by different ways. The purpose of the video broadcast of the VSV adjusts the camera easily, so that it can make tracking the target better. On the maritime cloud server, the purpose of the playing video is to have a clear understanding of the experiment site and analysis things what happened after that. Therefore, the image definition must be distinguished and should be enhanced before playing.

3.5. Video Storage Module. It is a part of the important functions of the system that the storage of video data during the experiment process, to analyze the situation of the experimental field after the experiment is possible. The maritime cloud server center is analysis and disposing center of the experimental data that has intense computing power and large storage space; it is appropriate to backup and long-term archival of experimental data. The transmission of data can be reduced by using the mode of maritime cloud server center storage. However, the data obtained by USV are transmitted by the wireless channel, and the noise and interference are unavoidable. After being processed a few steps, the data will increase the corresponding noise of process. The definition of video image is the most important index of the system, in order to archive the data of high quality and remove unnecessary noise and interference, the video data will be stored in the USV board monitoring platform.

4. Improved Hill Encryption Algorithm

The idea of Hill algorithm is to convert l cleartext letters into l ciphertext letters by a series of linear transformations, the decryption only requires one inverse transformation [11], and the key is the transformation matrix itself. Hill password is a part of the multiple-letter substitution codes and it is also called the matrix transformation password. The vector of cryptograph is $C = KM(\mathrm{mod}N)$

$$C = \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_l \end{bmatrix} \tag{1}$$

$$M = \begin{bmatrix} m_1 \\ m_2 \\ \vdots \\ m_l \end{bmatrix} \tag{2}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{3}$$

$$K = \left(k_{ij}\right)_{l\times l} = \begin{bmatrix} k_{11} & k_{12} & \dots & k_{1l} \\ k_{21} & k_{21} & \dots & k_{2l} \\ \vdots & \vdots & & \vdots \\ k_{l1} & k_{l2} & \dots & k_{ll} \end{bmatrix} \tag{4}$$

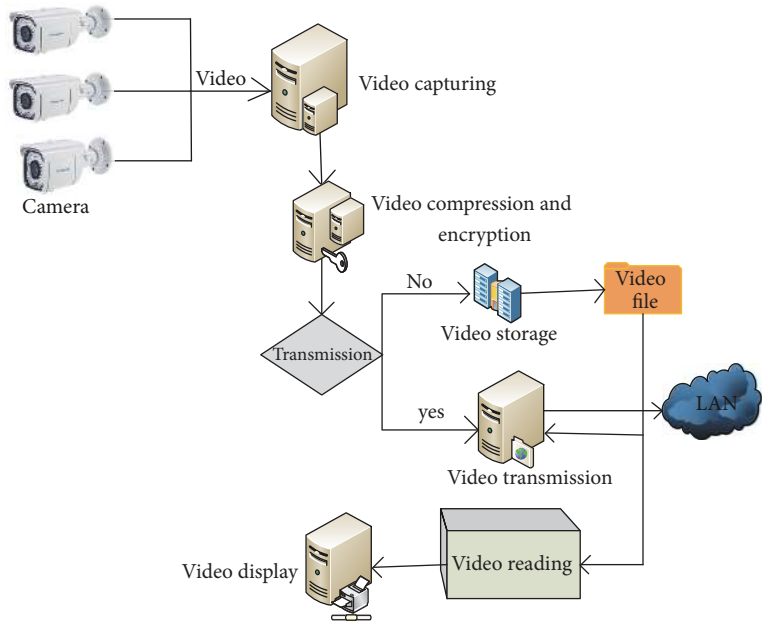

Figure 2: Flowchart of information processes.

In the formula, C is ciphertext and M is cleartext and the key K is an invertible matrix. The decryption formula is $M = K^{-1}C(\text{mod}N)$. All the arithmetic operators are performed under the mode of $N = 26$.

Example 1. Suppose the key $K = \left[\begin{smallmatrix} 6 & 7 \\ 3 & 8 \end{smallmatrix}\right]$; while the encryption comes true by using the Hill password, according to the above calculation we can get a result that $K^{-1} = \left[\begin{smallmatrix} 8 & 19 \\ 23 & 6 \end{smallmatrix}\right]$. Suppose that the "good" is cleartext to be encrypted, then the cleartext is divided into two groups that (6,14) is "go" and (14,3) is "od". The process of encryption is

$$\begin{aligned} \begin{bmatrix} c_1 \\ c_2 \end{bmatrix} &= K \begin{bmatrix} m_1 \\ m_2 \end{bmatrix} = \begin{bmatrix} 6 & 7 \\ 3 & 8 \end{bmatrix} \bullet \begin{bmatrix} 6 \\ 14 \end{bmatrix} (\text{mod}26) \\ &= \begin{bmatrix} 134 \\ 130 \end{bmatrix} (\text{mod}26) = \begin{bmatrix} 4 \\ 0 \end{bmatrix} \\ \begin{bmatrix} c_3 \\ c_4 \end{bmatrix} &= K \begin{bmatrix} m_3 \\ m_4 \end{bmatrix} = \begin{bmatrix} 6 & 7 \\ 3 & 8 \end{bmatrix} \bullet \begin{bmatrix} 14 \\ 3 \end{bmatrix} (\text{mod}26) \\ &= \begin{bmatrix} 105 \\ 66 \end{bmatrix} (\text{mod}26) = \begin{bmatrix} 1 \\ 14 \end{bmatrix} \end{aligned} \tag{5}$$

The result of encryption is "EABO". The process of decryption is

$$\begin{aligned} \begin{bmatrix} m_1 \\ m_2 \end{bmatrix} &= K^{-1} \begin{bmatrix} c_1 \\ c_2 \end{bmatrix} = \begin{bmatrix} 8 & 19 \\ 23 & 6 \end{bmatrix} \bullet \begin{bmatrix} 4 \\ 0 \end{bmatrix} (\text{mod}26) \\ &= \begin{bmatrix} 32 \\ 92 \end{bmatrix} (\text{mod}26) = \begin{bmatrix} 6 \\ 14 \end{bmatrix} \\ \begin{bmatrix} m_3 \\ m_4 \end{bmatrix} &= K^{-1} \begin{bmatrix} c_3 \\ c_4 \end{bmatrix} = \begin{bmatrix} 8 & 19 \\ 23 & 6 \end{bmatrix} \bullet \begin{bmatrix} 1 \\ 14 \end{bmatrix} (\text{mod}26) \\ &= \begin{bmatrix} 274 \\ 107 \end{bmatrix} (\text{mod}26) = \begin{bmatrix} 14 \\ 3 \end{bmatrix} \end{aligned} \tag{6}$$

Get the correct cleartext in the last.

4.1. Self-Invertible Matrix. In the encryption formula, K has inverse matrix K^{-1} and $(K^{-1}K)M = M = K^{-1}C(\text{mod}26)$, which is possible to realize the decryption. Essentially, using the invertible matrix K is important when you encrypt/decrypt. How do you see a matrix can be invertible? It depends on the determinant that is [12] nonzero (all of the above operations are performed under mode $N = 26$). So we know that the invertible matrix K has the inverse of the mode of $N = 26$, only if $GCD(\det K, 26) = 1$. Here, we use the $GCD(x, y)$ to denote the largest common divisor of the integer x and the integer y, using $\det K$ or $|K|$ to represent the determinant of the matrix K. The Hill encryption algorithm is applied to the image matrix P to get the corresponding Hill image encryption algorithm; the encryption process is $C = E_k(P) = K \bullet P$, and decryption process is $P = D_k(C) = K^{-1} \bullet C = K^{-1} \bullet K \bullet P = P$.

The basis of the algorithm is as follows.

If matrix A satisfies $A = A^{-1}$, then A is called a self-invertible matrix. Assumptions

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & \vdots & a_{nn} \end{bmatrix} \tag{7}$$

It is $n \times n$ self-invertible matrix, n is even, and suppose $n = 2$, then it is written as

$$A = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix} \tag{8}$$

In the formula, $A_{11}, A_{12}, A_{21}, A_{22}$ are $(n/2) \times (n/2)$ matrices. Result from the self-reversibility of A are

$$A \bullet A = A \bullet A^{-1} = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix} \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix} = I \tag{9}$$

Result from formula (8) is

$$A_{12}A_{21} = I - {A_{11}}^2 = (I - A_{11})(I + A_{11}) \tag{10}$$

According to formula (9), $|A_{12}|$ is a factor of $|I - {A_{11}}^2|$ and $|A_{21}|$ is another factor. Suppose there is a constant k

$$A_{12} = k(I - A_{11}) \tag{11}$$

Then

$$A_{21} = \frac{(I + A_{11})}{k} \tag{12}$$

From formula (11) we can get second matrix equations

$$A_{11}A_{12} + A_{12}A_{22} = 0 \tag{13}$$

When formula (10) is established, $|A_{11}|$ and $|A_{12}|$ will be exchanged

$$\begin{aligned} A_{11}A_{12} &= A_{11} \bullet k(I - A_{11}) = k(I - A_{11}) \bullet A_{11} \\ &= A_{12}A_{11} \end{aligned} \tag{14}$$

Formulae (13) to (12) obtain

$$A_{12}A_{11} + A_{12}A_{22} = A_{12} \bullet (A_{11} + A_{22}) = 0 \tag{15}$$

while $A_{12} \neq 0$ get the result

$$A_{11} + A_{22} = 0 \tag{16}$$

The self-reversible matrix algorithm is obtained.

The algorithm steps are as follows:

(1) Choose $(n/2) \times (n/2)$ matrix A_{22} arbitrarily.

(2) Get the result by a series of calculations that $A_{11} = -A_{22}$.

(3) Take $A_{12} = k(I - A_{11})$ or $k(I + A_{11})$ and k is a prime number.

(4) Count $A_{21} = (I - A_{11})/k$ or $A_{21} = (I + A_{11})/k$.

(5) Merge into a complete matrix.

4.2. Improved Hill Encryption Scheme. The steps of improved Hill encryption algorithm are as follows.

Step 1. $m \times m$ self-reversible matrix is generated as the key matrix of this algorithm.

Step 2. Divide the original image into $m \times m$ block image.

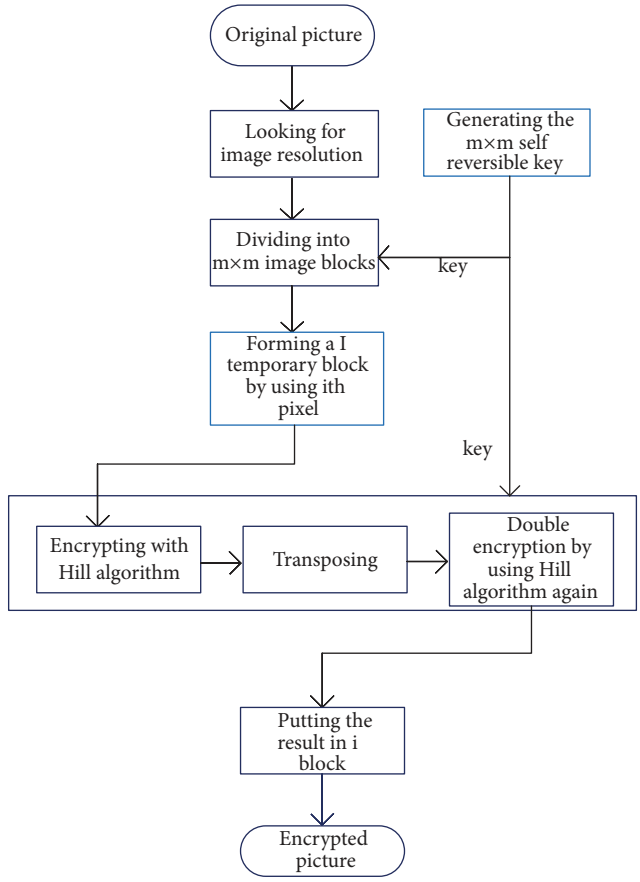

Figure 3: Flowchart of encryption.

Step 3. The i pixels of each image block will be grouped together and made up $m \times m$ temporary image block, it is convenient for future encryption operation.

(1) The temporary image matrix is encrypted with the key matrix A.

(2)Transpose the encrypted image matrix and double-layer encrypting the matrix.

Step 4. Putting the obtained matrix into the ith position of the final encryption matrix.

The process of decryption is the reverse process of encryption; the block diagram of the specific encryption algorithm is shown in Figure 3.

4.3. Security Analysis of Hill Algorithm. The key conditions of Hill encryption algorithm are character information and digital correspondence table and encryption matrix. Character information and number correspondence table representation: the larger the order of the encryption matrix is, the more difficult it is to decipher and the amount of calculation. The definition of the encryption matrix and the solution of the matrix are also very important to [13] encryption and decoding of the algorithm. From the point of cryptanalysis code, using traditional passwords to encrypt video has a lot of drawbacks; the broken translator can sum up the analogous

Table 1: Adjacent pixel.

direction	Artwork	Hill encryption	Article encryption
level	0.902985	0.329121	-0.005825
vertical	0.874309	0.227804	0.008831
diagonal	0.856915	0.173428	-0.030353

rules from the statistical string frequency and find out the exit of cryptanalysis. With the rapid development of science and technology, the deciphering time is less than before. But Hill encryption algorithm [14] uses matrix multiplication and inversion in linear algebra, it is better to resist frequency analysis, and it is difficult realizing the decoding. Hill encryption algorithm has set up three handicaps for the translator, which is incomprehensible to decipher. Because you do not know anything about that dimension variables of the text conversion, order of the corresponding letters, access method of the encryption matrix, if you want to decipher the code you should guess the three things correctly at least. But it is difficult to guess correctly at the same time. There is no password that can not be broken completely, and the Hill algorithm is no exception. Generally speaking, it is difficult decoding that only knows the attack of ciphertext, but it is easy to be broken by using attack of cleartext. Assume that the opponent already knows the value L and it also mastered l different tuples L at least. $M_i = \begin{bmatrix} m_{1i} \\ m_{2i} \\ \vdots \\ m_{li} \end{bmatrix}$, $C_i = \begin{bmatrix} c_{1i} \\ c_{2i} \\ \vdots \\ c_{li} \end{bmatrix}$, $1 \le i \le l$ The conditions were fulfilled that $C_i = E(M_i, K) = e_K(M_i)(1 \le i \le l)$. Defining two matrices that are $M = (m_{ij})_{l\times l}$ and $C = (c_{ij})_{l\times l}$, then has a matrix equation $C = K \bullet M(\text{mod}26)$. In the formula, $l \times l$ matrix K is an unknown key. If the M is reversible that can be calculated, $K = C \bullet M^{-1}(\text{mod}26)$. Thus the encryption algorithm is broken (if M is not reversible, we must try another cleartext-ciphertext pair). From the overall result Hill algorithm is still a simple and efficient algorithm.

5. Experimental Results and Analysis

In order to test the correlation between the two pixels adjacent to the vertical, adjacent, horizontal, the following tests are performed. Firstly, 1000-3000 pairs of pixels adjacent to the horizontal, vertical, and diagonal direction are randomly selected from the graph, and the correlation formula is used to calculate the correlation [15].

$$r_{xy} = \frac{\text{cov}(x, y)}{\sqrt{D(y)}\sqrt{D(x)}} \tag{17}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \tag{18}$$

$$\text{cov}(x, y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))((y_i - E(x)) \tag{19}$$

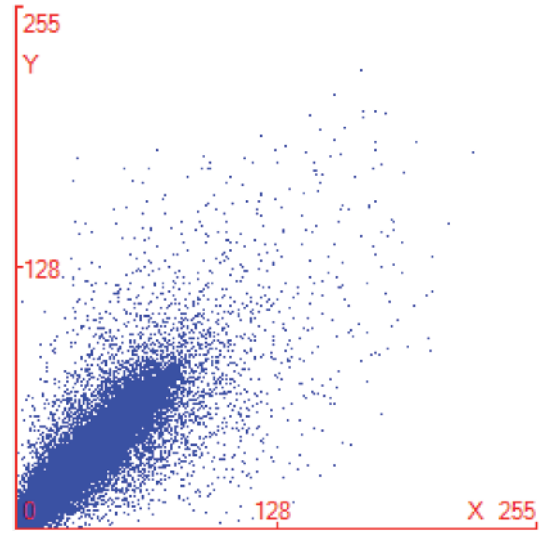

Figure 4: Correlation distribution diagram of original image.

In the formula, x and y are the gray values of two adjacent pixels in the image. $E(.)$, $D(.)$, and cov(.)are the expectation, variance, and covariance, respectively, and r is the correlation [14] coefficient of adjacent two pixels. The higher the value of its value is close to 1, the higher the correlation of adjacent pixels is. If images were encrypted by Hill self-invertible matrix encryption algorithm and improved algorithm, respectively, then compare the correlation between adjacent pixels in 3 directions.

$$UACI = \frac{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}|C_1(i, j) - C_1(i, j)|}{255 \times M \times N} \times 100\% \tag{20}$$

The related data of Table 1 show that the adjacent pixels of the original image are large data, the correlation coefficient is close to 1 that can be seen, the adjacent pixels are highly correlated, the pixels correlation of traditional Hill encryption algorithm is around 0.2, but improved algorithm is more precise in reducing the correlation of adjacent pixels, making the size of data close to 0. From the correlation of adjacent pixels that improved encryption algorithm is much better than traditional Hill encryption algorithm.

Figures 4 and 5 represent the correlation distribution diagrams of two horizontal adjacent pixels in the original and traditional Hill encryption images, and the correlation distribution of Figure 5 is more diffuse than Figure 4, but the correlation distribution between the original image and the traditional Hill encryption image is not obvious enough. Figure 6 shows the improved algorithm encryption image, the

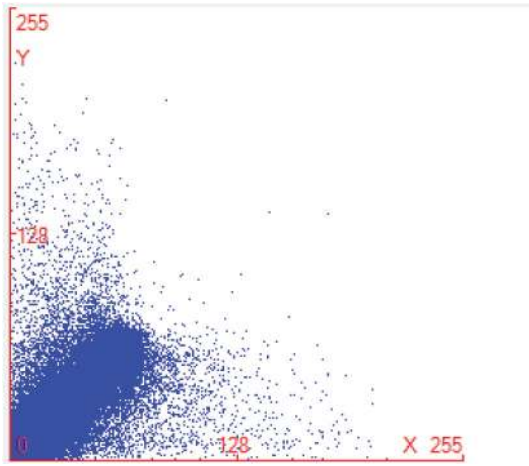

Figure 5: Correlation distribution of Hill encryption algorithm.

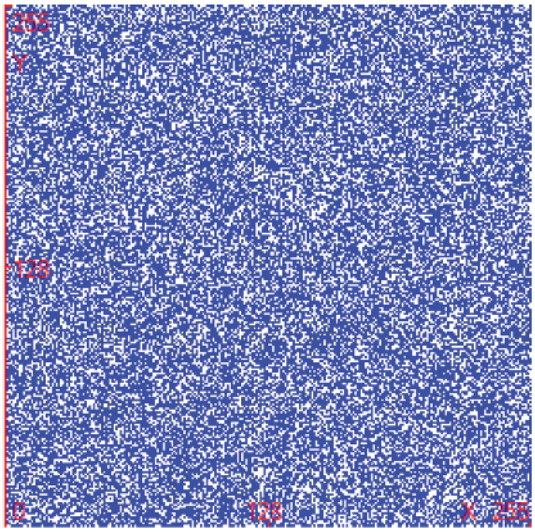

Figure 6: Correlation distribution of improved encryption algorithm.

comparison [16] between Figure 6 and Figure 5 shows that the correlation distribution is separate completely. From the analysis of the distribution degree of correlation graph, it is shown that the improved encryption algorithm is better than traditional Hill encryption algorithm.

5.1. Histogram Analysis of Encrypted Image. The variance is used to evaluate the consistency of histogram distribution and indicate the degree of dispersion between the histogram and its average value; the consistency of the distribution is expressed by the size of variance value. The smaller the variance the more uniform the distribution. The histogram of image is represented by $hist_i$, and the formula of variance is

$$S = \frac{1}{256}\sum_{i=0}^{255}\left(hist_i - aver\right)^2 \tag{21}$$

Figure 7: Original image.

and the *aver* is

$$aver = \frac{1}{256}\sum_{i=0}^{255} hist_i \tag{22}$$

The pixel value can be distributed evenly that, in the range of (0-255) after encryption, the uniform distribution of gray histogram will be regarded as the ideal state. From the above three images, it is found that the histogram (Figure 8) of the original image (Figure 7) is uneven, the uniformity of distribution is not ideal, the distribution effect (Figure 10) of the traditional Hill encryption image (Figure 9) has not been improved obviously, which has poor performance, and the pixels correlation of the image is not weakened. Compared with the traditional Hill encryption histogram, the histogram (Figure 12) of the improved algorithm encryption image (Figure 11) is more concentrated and more gentle. The value of the variance is obviously smaller than variance of the traditional Hill encryption algorithm, which weakens the correlation greatly and its result is ideal.

5.2. Information Entropy and Diffusivity Test. **Information entropy** is a concept used to measure the amount of information in information theory, which contains information content of an image, the system is more orderly that information entropy is more low. The information entropy of the image is

$$H\left(m\right) = -\sum_{i=0}^{L-1} p\left(m_i\right)\log_2 p\left(m_i\right), \qquad \sum_{i=0}^{L-1} p\left(m_i\right) = 0 \tag{23}$$

L and mi in the formula indicate that gray value is mi and description is L; P_{mi} indicates the probability of the appearance of gray value. When the probability that gray value appears in the image is equal, information entropy of

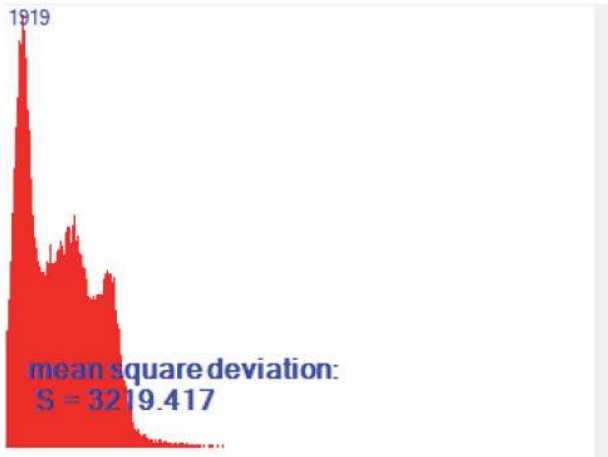

Figure 8: Histogram of original image.

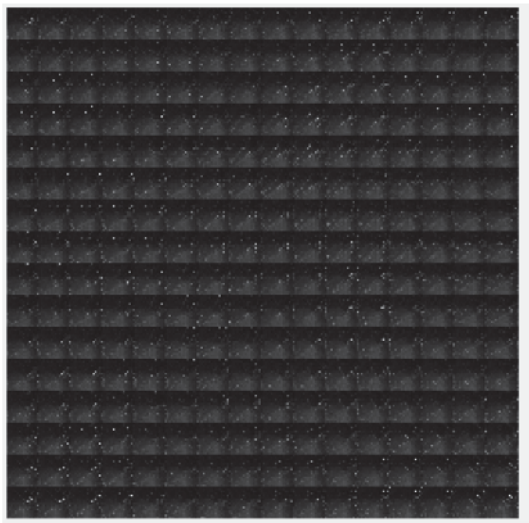

Figure 9: Hill encryption image.

the image is the largest, and its gray distribution is identical. When information entropy is equal to 8, that proved the fact that the random distribution of images is more ideal.

Diffusion is an important nature in the encryption algorithm that is proposed by Shannon in a document; an excellent encryption system must have good diffusivity. The meaning is that when a bit is changed in the original image, the encryption image will be changed in an unpredictable way. The diffusivity of the image encryption algorithm indicates that the output pixels of the encrypted image [17] should be dependent on the input pixels of the original image in a very complicated way, which can resist the attacker's analysis of the algorithm. Attackers usually make small changes to the original image and then use the algorithms used as attackers to encrypt the original and modified images and compare the relationship between the original and the encrypted images by comparing two images. This kind of attack becomes a difference attack [18]. One pixel of the original image is modified by the attacker; looking at the changes in the result,

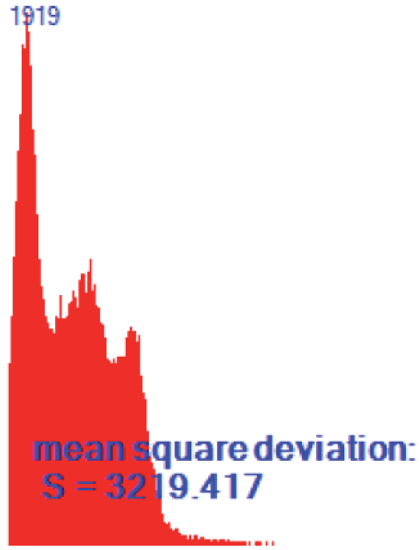

Figure 10: Histogram of Hill encryption image.

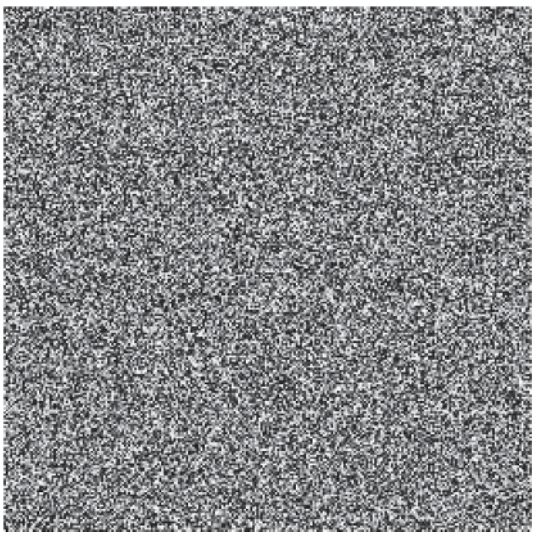

Figure 11: Improved Hill encryption image.

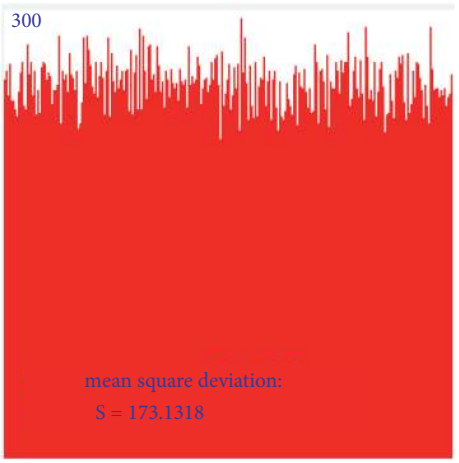

Figure 12: Histogram of improved Hill encryption image.

Table 2: Analysis of test results.

information	Artwork	Hill encryption	Article encryption
entropy	6.234655	6.234655	7.997266
NPCR	0.00	0.00001526	0.00024424
UACI	0.00	0.000015019	0.001794146

it is possible for attacker to find a relationship between the original image and the encrypted image. If a small change in the original image can cause significant changes in the effects of diffusion and chaos, the efficiency of the differential attack is very low and the attack is invalid. In order to verify the influence of a pixel change in the entire encrypted image, two measurement methods are commonly used: one is pixel change rate and the other is uniform average change intensity. Two encrypted images are represented by C_1 and C_2, respectively, only one pixel is different in their corresponding original images, and the gray values of images C_1 and C_2 at coordinates (i, j) are represented by $C_1(i, j)$ and $C_2(i, j)$, respectively.

$$D(i,j) = \begin{cases} D(i,j) = 0, & C_1(i,j) = C_2(i,j) \\ D(i,j) = 1, & C_1(i,j) = C_2(i,j) \end{cases} \tag{24}$$

The pixel change rate ($NPCR$) is defined as

$$NPCR = \frac{\sum_{i=0}^{M-1} \sum_{j=0}^{N-1} D(i,j)}{M \times N} \times 100\% \tag{25}$$

In the formula, M is width and N is height of images $C1$ and $C2$. The meaning of $NPCR$ is to calculate the percentage of different pixels in two images. The uniform average change intensity $UACI$ is defined as

$$UACI = \frac{\sum_{i=0}^{M-1} \sum_{j=0}^{N-1} |C_1(i,j) - C_1(i,j)|}{255 \times M \times N} \times 100\% \tag{26}$$

From Table 2, we can know that the information entropy of the original image is equal to 6; the entropy of the traditional Hill encryption image is about 6. It is shown that the traditional Hill encryption algorithm does not make a significant change in the probability of the random distribution of the image, and there is no more agreement on the gray distribution. Information entropy is more small that the image is more orderly and the probability of the image random distribution is more small. Using the improved encryption algorithm to encrypt image, the information entropy is increased from the original data to 8, the information entropy is more great, random distribution of the image is more ideal, the more consistent in the gray distribution and the encryption effect is more ideal. From the pixel change rate, we can learn that the results of the improved algorithm are more large than the traditional Hill algorithm on the numerical value, and the results of the uniform average change intensity have a little difference [19].

6. Conclusion

In this paper, the tool used in this experiment is Visual Studio 2015, using the *c#.NET* language. We introduced the video monitoring system of the USV and the module of the system briefly, aiming at the favorable security and efficient efficiency of traditional image encryption technology; an improved algorithm is proposed based on Hill encryption algorithm. The algorithm is that a $m \times m$ self-invertible matrix is generated as the key matrix of this algorithm, then dividing the original image into $m \times m$ block image. The ith pixels of each image block will be grouped together and make up a temporary $m \times m$ image block, it is convenient for future encryption operation [20–23]. The temporary image matrix is encrypted with the key matrix A, transposing the encryption image matrix and double- layer encrypting the matrix and putting the obtained matrix into the ith position of the final encryption matrix. We use double-layer encryption strategy to decide the degree of scrambling and enhance the security of the encryption system. Results of experiments show that the algorithm has high efficiency of scrambling and the disorderly effect is uniform and the correlation of adjacent pixels is small, which changes the statistical information of the image and that is more ideal in the random distribution of the image and gray level. Through the analysis of its performance theory and experimental results, it has been shown that the improved algorithm is more successful than traditional Hill encryption algorithm and has great developmental potentialities. From the influence of pixel change rate and uniform average change intensity of encrypted image, the algorithm has not greatly improved the pixel change rate and value is too small that does not reach more than 0.9, they can improve by changing the length and width of the image. Therefore, considering the improvement in these two aspects will be a direction for the future.

Data Availability

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

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported in part by Research Project for FY2017 of International Association of Maritime Universities, China Postdoctoral Science Foundation under Grant 2015T80238, Natural Science Foundation of China under Grants 61771086 and 61401057, the Military Commission Equipment for the 13th Five-Year Field Fund Project under Grant 61403120402, Dalian Outstanding Young Science and Technology Talents Foundation, Natural Science Foundation of Liaoning Province under Grant 201602083, Science and Technology Research Program of Liaoning under Grant L2014213, Dalian Science and Technology Project under

Grant 2015A11GX018, Research Funds for the Central Universities 3132018144, 017180327, and 01760325, and Dalian High-level Innovative Talent Project under Grant 2016RQ035.

References

[1] K. Mani and R. Mahendran, "Generation of Key Matrix for Hill Cipher Encryption Using Classical Cipher," in *Proceedings of the 2nd World Congress on Computing and Communication Technologies, WCCCT 2017*, pp. 15–64, February 2017.

[2] M. Lakhera, M. M. S. Rauthan, and A. Agarwal, "Securing biometric template using double hill cipher with self-invertible key and random permutation of pixels locations," in *Proceedings of the 2nd IEEE International Conference on Next Generation Computing Technologies, NGCT 2016*, pp. 814–817, India, October 2016.

[3] A. N. Borodzhieva, "MS excel-based application for encryption and decryption of English texts with the hill cipher on the basis of 3×3-matrix," in *Proceedings of the 25th International Scientific Conference Electronics, ET 2016*, Bulgaria, September 2016.

[4] J. Zou and T. Weng, "A new image encryption instant communication method based on matrix transformation," *Smart Innovation, Systems and Technologies*, vol. 63, pp. 321–329, 2017.

[5] D. Xu, R. Wang, and Y. Q. Shi, "An improved scheme for data hiding in encrypted H.264/AVC videos," *Journal of Visual Communication and Image Representation*, 2015.

[6] T. Iakymchuk, A. Rosado-Munoz, M. B. Mompean, J. V. F. Villora, and E. O. Osimiry, "Versatile Direct and Transpose Matrix Multiplication with Chained Operations: An Optimized Architecture Using Circulant Matrices," *IEEE Transactions on Computers*, vol. 65, no. 11, pp. 3470–3479, 2016.

[7] M. Haj and M. Qatawneh, "Parallel Hill Cipher Encryption Algorithm," *International Journal of Computer Applications*, vol. 179, no. 19, pp. 16–24, 2018.

[8] T. Sivakumar and R. Venkatesan, "A novel image encryption approach using matrix reordering," *WSEAS Transactions on Computers*, vol. 12, no. 11, pp. 407–418, 2013.

[9] X. Liu, Z. Wei, and C. J. Carter, A novel image encryption approach using block based transformation and random phase encoding,.

[10] S. Muttoo, D. Aggarwal, and B. Ahuja, "A Secure Image Encryption Algorithm Based on Hill Cipher System," *Bulletin of Electrical Engineering and Informatics*, vol. 1, no. 1, 2012.

[11] M. A. Aljanabi, N. A. Shnain, and S. F. Lu, "An image similarity measure based on joint histogram — Entropy for face recognition," in *Proceedings of the 3rd IEEE International Conference on Computer and Communications (ICCC '17)*, pp. 1626–1631, Chengdu, December 2017.

[12] L. J. Ontanon-Garcia, M. Garcia-Martinez, E. Campos-Canton, and S. Celikovsky, "Grayscale image encryption using a hyperchaotic unstable dissipative system," in *Proceedings of the 2013 8th International Conference for Internet Technology and Secured Transactions (ICITST)*, pp. 503–507, London, United Kingdom, December 2013.

[13] F. Gmira, S. Hraoui, W. Sabbar, and A. Jarrar Oulidi, "Image transaction encryption based on a dynamic upswing of hill cipher and JPEG compression," *International Journal of Imaging and Robotics*, vol. 17, no. 3, pp. 14–17, 2017.

[14] Cellular-news, "Maritime WiMAX Network Launched in Singapore," http://www.cellular-news.com/story/29749.php.

[15] M. G. V. Prasad and P. Sundarayya, "Generalized self-invertiblekey generation algorithm by using reflection matrix in hill cipher and affine hill cipher," in *Proceedings of the IEEE Symposium Series on Computational Intelligence*, vol. 8, pp. 11–23, 2018.

[16] R. Huang and C. Lu, "Research of H.264 video transmission encryption technology based on blowfish algorithm," in *Proceedings of the 4th International Conference on Computer Science and Network Technology, ICCSNT 2015*, pp. 931–935, China, December 2015.

[17] S. S. Giradkar and A. Bhattacharya, "Securing compressed video streams using RC4 encryption scheme," in *Proceedings of the Global Conference on Communication Technologies, GCCT 2015*, pp. 640–644, India, April 2015.

[18] R. Bhardwaj, "Enhanced encrypted reversible data hiding algorithm with minimum distortion through homomorphic encryption," *Journal of Electronic Imaging*, vol. 27, no. 02, p. 1, 2018.

[19] N. Zhang, N. Cheng, N. Lu, X. Zhang, J. W. Mark, and X. Shen, "Partner selection and incentive mechanism for physical layer security," *IEEE Transactions on Wireless Communications*, vol. 14, no. 8, pp. 4265–4276, 2015.

[20] D. Chen, N. Zhang, Z. Qin et al., "S2M: A Lightweight Acoustic Fingerprints-Based Wireless Device Authentication Protocol," *IEEE Internet of Things Journal*, vol. 4, no. 1, pp. 88–100, 2017.

[21] J. Wu, K. Ota, M. Dong, J. Li, and H. Wang, "Big Data Analysis-Based Security Situational Awareness for Smart Grid," *IEEE Transactions on Big Data*, vol. 4, no. 3, pp. 408–417, 2018.

[22] L. Kuang, L. T. Yang, J. Feng, and M. Dong, "Secure Tensor Decomposition Using Fully Homomorphic Encryption Scheme," *IEEE Transactions on Cloud Computing*, vol. 6, no. 3, pp. 868–878, 2018.

[23] M. Tao, K. Ota, M. Dong, and Z. Qian, "AccessAuth: Capacity-aware security access authentication in federated-IoT-enabled V2G networks," *Journal of Parallel and Distributed Computing*, 2017.