Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 10, October 2021: 4309-4321

Research Article

SVC BASED ENCRYPTION METHOD FOR PRIVACY PROTECTION IN SURVEILANCE VIDEO

T. Sugirtha raj [a] , V.Subbiah [a] , P. Aathi sankar [a] , Dr. S.Rajagopal [a]

[a] - Department of Information Technology, National Engineering College, K.R. Nagar, Kovilpatti, Thoothukudi (Dt), Tamilnadu 628503, India

ABSTRACT

A multimedia video surveillance system main aim is to offer security of people who appear in the surveillance video. However, due to the nature of video surveillance, video will be stored in the server as original format of the video which is not safe. However, many cryptographic algorithm and techniques now applying in video surveillance to encrypt the video, e.g., AES and DES, but that are not suitable and efficeient for surveillance videos to encrypt the video because size of the video is large. In our method we introduce SVC based video compression technique and light weighted encryption technique in the existing video surveillance system. In our method, we propose bitstream-oriented layered cellular automata(LCA) encryption scheme for SVC. Using our approach, the compressed video organized as 8-layer cellular automata (CA) then it will converted into a binary block. The simple 8X8 layer evolution technique and layered shift transformation based on the hierarchy generated key make the particular video encryption efficiently. In order to offer more security, as well as achieving light weight requirement, we use hierarchical key management technique. It generate random key for shift transformation. Finally the encrypted video stored in the cloud. The experiment analysis and final outputs indicate that the proposed model achieves a high-security level, and light weight requirements for video surveilance.

Keywords. SVC , layered cellular automata , shift transformation, cloud

I.INTRODUCTION

With the development of internet and cloud computing devices, the application of video surveillance systems have significantly increased in the last three decades because the explosive growth of multimedia computing, all the videos and information stored in cloud or server only. Security in cloud computing is a major concern. To over come this problem videos in cloud should be stored in encrypted format. To restrict client from accessing the shared data directly,we can convert the video into another form so that it will be stored in the cloud as very secure way. Encryption helps to protect data from being compromised. You need a secure way to immediately access your data. cryptographic encryption technique ensures your data and applications are readily available to all authorized users. In today Cloud computing provide various services like paas, iaas, saas through the Internet. These services include various tools like data storage, networking devices, and software services, servers, databases. Rather than keeping all records on a secondary storage or local storage device in a computer, cloud-based storage makes it possible to save all data and videos to a remote or centralized database. Video encryption is essential techniques for the all users who are worried about the safety and privacy of the records they store in the cloud storage devices.

However, most of the known cryptographic techniques are not suitable to encrypt video because of their large computational costs. In addition, normal encryption technique is not efficient for hardware implementation due to continuous use of surveillance. Therefore, the lightweight and hardware friendly encryption method is needed to encrypt the video.

Some researchers applied one dimensional (1D) cellular automata to image encryption schemes , because the evolution of 1D cellular automata is not efficientfor represent image pixel matrix. Now a days two dimensional cellular automata pixel matrix can represent an image more efficiently and clearly, a 2D cellular automata is more suitable for both video and image encryption because its easy to develop and reduce developmental cost. In this method, each value in a 8X8 layer pixel matrix will convert into a binary sequence. Note that the binary representation of an image is a composition of some binary matrices, which implicates an image can be viewed as a combination of some independent 2D CAs.

We introduce a combination of svc and LCA based encryption method that will overcome the above addressed problems efficiently and suitable for all the cloud-computing video applications. Specifically, it supports provide strong video protection. against malicious users and untrusted cloud. In our method, each compressed video will be organized as 8X8 layer pixel value then it will be converted into a 8X8 layer binary block and then set as the initial states for a LCA proposed in the paper. Thereafter, the LCA uses its reversible rules and simple transformations model for state transitions. The final state data of the LCA is again converted into original form and saved as the encrypted format in cloud. All surveillance video which are coming from different surveillance camera are encrypted independently and stored in the cloud.

- The video's are encrypted and stored at the cloud for an on-demand service required by the authenticated users, which makes the proposed process both effective and security .

- The simple 8X8 layer evolution technique and layered shift transformation based on the hierarchy generated key make the particular video encryption efficiently.

- A randomized key is generated and it will show different encryption results, and thus the algorithm is able to resist the known plaintext attacks. Experimental results show that our approach has desirable security effects, which ensure that the attackers cannot the derive private information from the encrypted video's without the key.

This paper is categorized as follows. In Section II related works, In Section III we introduce the preliminaries of our approach, including the concepts of cellular automata, elementary cellular automata and layered cellular automata.. In Section IV problem statement, In section V we present the lightweight LCA based encryption, followed by the experimental results in Section VI.

II. RELATED WORK:

A. LCA method

In order to overcome and eliminate off-line brute-force attacks in existing surveillance video xing zhang et al [1] proposed an encryption and decryption design process and implementation which make more efficient for existing video surveillance systems. Privacy protection in surveillance and security of surveillance captured videos is an important issue because of the pervasive surveillance cameras. However, many cryptographic algorithm and techniques now applying in video surveillance to encrypt the video, e.g., AES and DES, but that are not suitable and efficient for surveillance videos to encrypt the video because size of the video is large. They introduce ROI based LCA encryption method. In this method first picture is organized as 8X8 layered pixel matrix then ROI extraction technique applied to the layer then it will be converted into original format. The surveillance video without RoIs or without encryption can be watched real-time by admin or any user on-line with authentication. Theoretical experiment analyses and experiment results show that our approach is both light weight, effective and offer more security.

B. SVC Video format

In [2] Cheng Xu et al propose a format compliant SVC(scalable video coding) encryption scheme , Terminals with diverse technological specifications, heterogeneous network environment, large video size and personalized user requirements raise new challenges to streaming media services. Solutions for this problem is newly video compression format technique SVC/H.264[10] (SVC; designed to compress original video size to lower level video size that is it convert high bitstream into a multilayer video stream according to the user requirements) have been proposed.. In the article, they introduce a bitstream-oriented based 8X8 LCA scheme for scalable video coding bitstream. According to the multilayer bitstram code structure of scalable video coding, the bitstream of the picture or video is separated and encrypted, respectively, by rearranging the abstraction layered unit of SVC bitstream. This offers security and more protection for the layer characteristic of SVC. In order to provide sufficient protection and security for videos, as well as achieving improved computational efficiency and cost reduction, we use different cryptographic algorithms it start with base layer and enhancement layers according to its requirements given by the user. The base layer offer and provide high-security encryption algorithms, like block cipher, to ensure security for videos. Each enhancement layer is encrypted with a different random generated key through the stream cipher with low computational complexity, providing layered control of the video. With this, they introduce a hierarchical key management method to implement layered access control according to the principle of hierarchical dc wallet (H-D wallet) it generate random key to resist attacks. Our scheme can be applied to the all user-level distinction in video on demand ,and video surveillance systems in IoT ,it provide more security. The experiment results indicate that the proposed method and process achieves a high-security level, computational complexity and low compression cost.

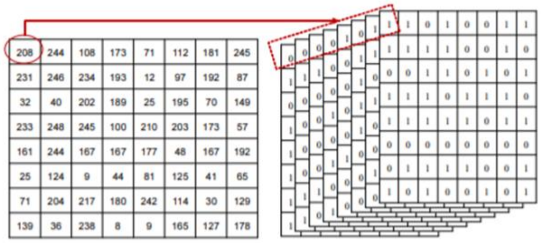
c. cloud security:

In [3] Yeswanth et al propose a method for Cloud security generally relates to managing, storing and processing of data over a network. The cloud provides mainly offers three services, platform as a service(paas), infrastrucure as a service(iaas), and software as a service(saas) using internet, based on the user's requirements. As it became a vital platform, many companies are building their infrastructure. This has increased the corresponding vulnerabilities and threats as these services are often provided by third parties. So, security of the cloud is a noteworthy issue for the cloud client because it should be access by only authorized user. On the other hand, should analyze efficiency of the cryptography algorithm is another problem. Efficiency of these cryptographic algorithms, based on the decryption process ,encryption process, encryption throughput and memory space for encryption by the algorithms for different sizes of file formats like images ,videos and text,. Further, increasing privacy of data stored in cloud by enhancing the security using encryption and decryption techniques like DES,RSA.

III. PRELIMINARIES:

A. LCA:

A layered cellular automata is a dynamic information processing system whose time and state are all independent. The CA consists of several cells arranged in a 8X8 layered matrix or 16X16 layered matrix. Each cell has its own state and all cells update their states and behavior simultaneously based on the random key generated. The pixel value of the image is arranged based on the 8X8 layered matrix. Then based on the generated key value state change their value, finally all the column value extracted and converted into original format system. When compared to 16X16 layered cellular automata 8X8 layered cellular automata suitable for video encryption process.



208	244	108	173	71	112	181	245
231	246	234	193	12	97	192	87
32	40	202	189	25	195	70	149
233	248	245	100	210	203	173	57
161	244	167	167	177	48	167	192
25	124	9	44	81	125	41	65
71	204	217	180	242	114	30	129
139	36	238	8	9	165	127	178

1	1	0	1	0	0	1	1
1	1	1	1	0	0	1	0
0	0	1	1	0	1	0	1
1	1	1	0	1	1	1	0
1	1	1	1	1	0	1	1
0	0	0	0	0	0	0	0
0	1	1	1	1	0	0	1
1	0	1	0	0	1	0	1

Figure 1: 8 X 8 Layer CA

B. Scalable Video Coding:

SVC is the another form or extension of the SVC/H.264 video compression method. A compressed video is formed from original video by dropping packets or reduce the bandwidth.The main objective of the scalable video encoding is that video contains two or more bitstream that themselves decoded or compressed into low quality bitstram.Compression method is one of the important process for video encryption. Because if the video size is large it takes more time to encrypt so we need to compress the video for encryption process. SVC is the best method for compression because its more effective than when compared to the other methods.

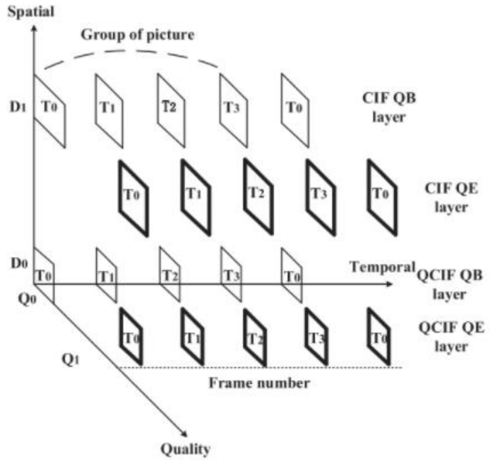


Figure 2 : SVC structure

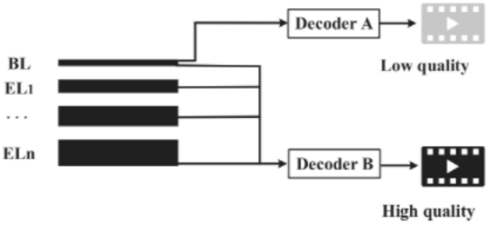


Figure 3: SVC bitstream extraction rules.

IV. PROBLEM STATEMENT:

As discussed above, encryption method should not be a process of creating encryption algorithms and organizing binary sequence. Algorithm should process all the images and encryption should tak place in very less time. Efficiency of cryptographic algorithms, based on the decryption time ,encryption time, encryption throughput and memory utilized for encryption by the algorithms for different sizes of file formats like image ,video and text, Current research is focused on compressing video format into smaller one then it takes less time to encrypt.

Our main security goal of this method is to provide strong protection and security against unauthorized users. In our system, 8 key is generated for all columns . After compression applied random key is generated and shift transformation is occurred. Finally extracted(Encrypted) Video Stored in the cloud.

ExistingSystem

In existing system, videos coming from different surveillance camera will be stored in storage device as original format of video which may be exploited by hackers. However, many cryptographic algorithm and techniques now applying in video surveillance to encrypt the video, e.g., AES and RSA, but that are not suitable and efficeient for surveillance videos to encrypt the video because size of the video is large.

V. PROPOSED SYSTEM:

In encryption process , pixel value is organized as binary block of 8X8 layered cellular automa. Then each video is compressed simultaneously .Since each layer of the LCA can be treated as a composition of a series of 1D CAs, we then apply generated key for transformation then each column change their state. In order to increase security and privacy, we also apply shift transformation in each row of the layer as well as in adjacent layers.

Encryption:

The video's are encrypted as follows.

STEP 1: Arrange pixel value from the original video into an 8-layer CA.

STEP 2: Apply SVC compression technique.

STEP 3: Initialization. Arrange the binary sequence from the compressed video into an 8-layer CA, and then let each layer contain 16 × 16 bits. Intra-layer shift. A half shift transformation is performed in each layer. For every row in a layer, only half cells change their states to the states of the cells at their adjacent row. Specifically, the cells at posterior columns will change their states and the other cells will keep static.

If there are k(k ∈ N) columns in each layer, the state of j th row in the l th layer at time t is (s^t ….,s^t). It will be shifted to the new state (s^{t+1}….,s^{t+1}) after an intra-layer half shift transformation, where

S^{t+1} = { s^t , 1<=j<=[k]

STEP 4 : Rule evolution. Each layer is treated as a composition of the rows of the 1D CAs with the same size. Thereafter, columns from different 1D cellular automa s change their values simultaneously. Finally, the encrypted video is formed by converting the final state of the 8X8 layered cellular automa into a pixel values.

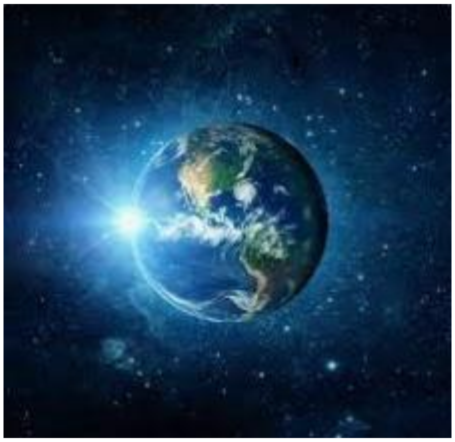


Figure 4: Before Encryption

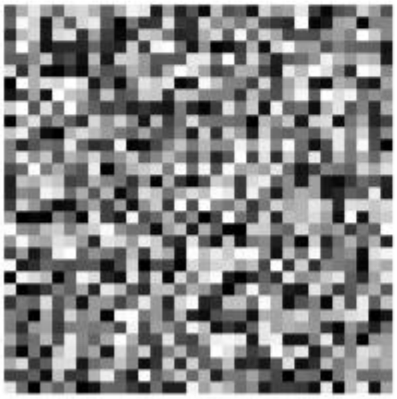


Figure 5: After Encryption

Encryption Algorithm:

Input : SVC Block SB, random sequence RS, iteration number N;

Output: Cipher block CB

```
SB <- Cell(SB)
For k=1 to N do
    SB <- Rule(SB,RS); //Rule evolution
    SB <- Intralayer(SB) //The intra-layer shift
    SB <- Intralayer(SB,RS) //The intra-row random shift
End for
CB <- Mat(SB)
Return CB;
```

Decryption:

In decryption process generated key is same as the encryption key. Shift transformation rule used for the encryption method but in decryption method reverse shift transformation process is applied. The binary sequence of an encrypted video is again formed as a 8X8 layered cellular automata. Forward shifting uses the rules selected by the decryption key. The inverse or reverse shift transformation is applied for decryption process it shift the each columns based on the generated key. The final 8X8 layered matrix converted into the pixel matrix by which to recover the video.

$$S^t = \{ s^{t+1} , 1<=j<=[k]$$

Decryption algorithm:

Input : SVC Block SB, random sequence RS, iteration number N;

Output: Cipher block CB

```
SB <- Cell(SB)
For k=1 to N do
        SB <- InIntrarowST(SB,RS) //The inverse procedure of intra-row random shift
        SB <- InIntralayerST(SB) //The inverse procedure of intra-row random shift
        SB <- InIntralayerST(SB) //The inverse procedure of intra-row random shift
SB <- Rule(SB,RS); //Rule evolution
End for
CB <- Mat(SB)
Return CB;
```

Hierarchical Key Management:

In our method , an 8X8-layered cellular automata and Scalable Video Coding bitstream requires N encryption keys, namely, K0–Kn−1. Based on the layered access control of this scheme, the user at the Ith layer with K0–Ki−1 cannot view the entire quality of the video sequence. Because there is no higher layer key Ki–Kn−1. Since each layer is assigned a different key, high-level users need to consume a lot of resources to store and manage all keys, and the loss of a key can also cause the imbalance of the layered access control.

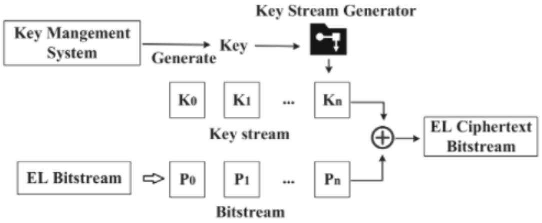


Figure 6: Key management system

$$M0 = E(C_0 + s^t , K)$$

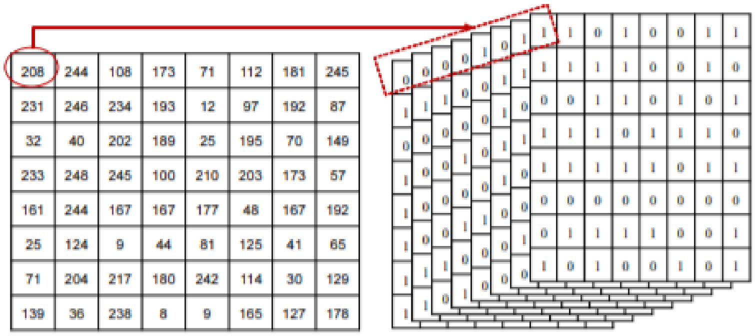
$$M_i= E(C_i + M_i , K) \ (i=1,2,\ldots\ldots\ldots)$$

where Ci is the base layer bitstream, K is the encryption key, , and Mi is the cipher text bitstream.. In order to reduce the computational cost, this article utilizes a lightweight stream cipher encryption scheme to encrypt each enhancement layer with different keys.

VI. IMPLEMENTATION

User Registration

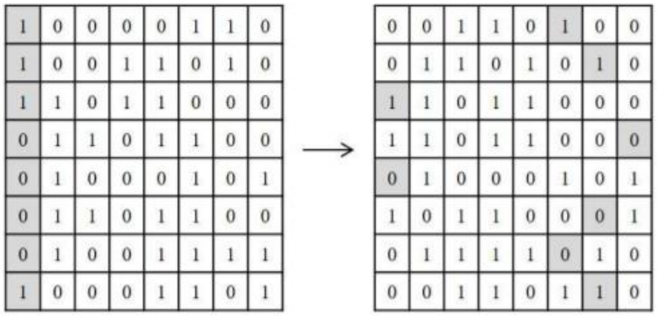
They are the owner and publisher of surveillance files and they should register their information in the server to store and retrieve the videos in the server. After they give and register, they should wait for some time to log into the server. After administrator of the server activates their registration, they can enter into the server. After they logged successfully, he gets secret key in their mail id. By giving that secret, user can enter into his home page.



208	244	108	173	71	112	181	245
231	246	234	193	12	97	192	87
32	40	202	189	25	195	70	149
233	248	245	100	210	203	173	57
161	244	167	167	177	48	167	192
25	124	9	44	81	125	41	65
71	204	217	180	242	114	30	129
139	36	238	8	9	165	127	178

1	1	0	1	0	0	1	1
1	1	1	1	0	0	1	0
0	0	1	1	0	1	0	1
1	1	1	0	1	1	1	0
1	1	1	1	1	0	1	1
0	0	0	0	0	0	0	0
0	1	1	1	1	0	0	1
1	0	1	0	0	1	0	1

Figure 7: Binary organization



1	0	0	0	0	1	1	0
1	0	0	1	1	0	1	0
1	1	0	1	1	0	0	0
0	1	1	0	1	1	0	0
0	1	0	0	0	1	0	1
0	1	1	0	1	1	0	0
0	1	0	0	1	1	1	1
1	0	0	0	1	1	0	1

0	0	1	1	0	1	0	0
0	1	1	0	1	0	1	0
1	1	0	1	1	0	0	0
1	1	0	1	1	0	0	0
0	1	0	0	0	1	0	1
1	0	1	1	0	0	0	1
0	1	1	1	1	0	1	0
0	0	1	1	0	1	1	0

Figure 8: Shift transformation based on hierarchy key generator

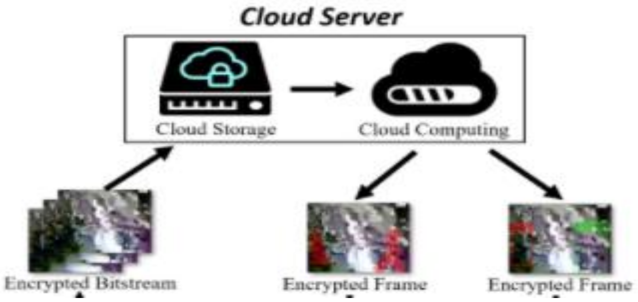


Figure 9:   Cloud structure

User Approval

Admin can execute this process. After user's entered their registration process, they cannot log into the server directly. Admin verifies and provides approval for each and every user separately. Then only their login will be activated. Based on their properties and personal information, he will approve the users who are registered.

Upload Surveillance Video

Data Owner can upload the surveillance videos which are coming different camera into the server. During this upload, it will generate the random id and store into the server. After that, he can encrypt the region of interest of video from particular camera randomly and store them into the server. It is used to maintain sensitive information securely in the cloud. Encryption can be done by A LCA-based reverse iterative encryption method.

Data Owner can download the surveillance videos. If they are not encrypted, the entire registered person can view and download the video. If they are encrypted using LCA algorithm, owner can use this video. If he wants to show and download, he should give corresponding key. By giving legitimate key, surveillance video will be decrypted, downloaded and viewed by data owner. During decryption stage, the pixel state of an encrypted video block is modified into an binary state. Forward shifting uses the rules selected by the decryption key. Thereafter, a inverse shift of the three different transformations mentioned above are performed.

Investigator

Investigator can register with in the server to access the captured video from the server. If he gives request to the server admin, he verifies his status and gets permission from data owner. After permission is granted by owner, he sends all the videos and if they are encrypted videos, admin will send corresponding keys along with encrypted surveillance videos. By giving generated keys, investigator can view the datas to examine

VII. EXPERIMENTAL RESULTS:

In our method we introduce SVC video compression technique and LCA based method in the video surveillance system. In our method, we propose bitstream-oriented layered cellular automata(LCA) encryption scheme for SVC. Using our approach, the compressed video organized as 8-layer cellular automata (CA) then it will converted into a binary block. The svc based compression technique and LCA method make the video encryption efficiently, and therefore it satisfies the lightweight requirements of surveillance videos.

Encryption techniques used for privacy protection in surveillance video should be privacy enough to prevent attacks deriving the important data from the encrypted videos. In our work, video's contain privacy informations are encrypted by using svc and LCA method. Several statistical experiments and measurements are used to analyze the security of our approach.

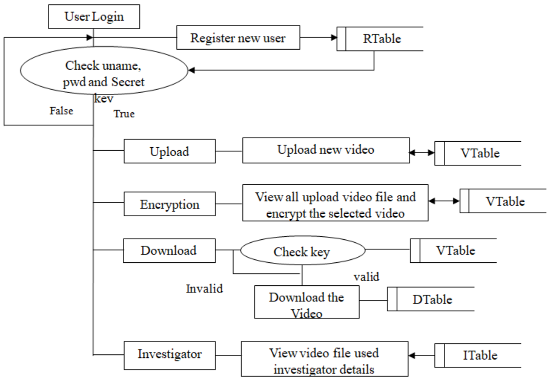


Figure 10: Workflow

VIII. Security and performance analysis:

Encryption algorithm used for privacy protection in surveillance video.It should be secure enough to prevent any attacks.

Several statistical experiments and measurements are used to analyze the security of our approach.

A. Information Entropy:

Information entropy process is an important measurement for the gray value distribution in an image. The information entropy of an image I is defined as follows:

$$E(I) = - \sum r(y_i)\log2r(y_i),$$

where , yi is the i th gray value in the image I, r(yi) is the occurrence probability of yi r , and i r(yi) = 1.

B. Correlation of adjacent pixels:

Correlation test of the adjacent pixels is an important statistical method to evaluate the diffusion and confusion of an encryption algorithm. Encrypted videos should have an almost zero correlation between the adjacent pixel value, whereas the plain image should present a strong correlation. To perform a correlation and adjacent test on an images, we randomly choose 500 pairs of adjacent pixels in vertical, diagonal and horizontal directions from a plain image and its cipher image, respectively. We then calculate the correlation coefficient, where the correlation and adjacent coefficient is defined as follows:

$$R_{xy}= \frac{cov(x,y)}{D(x).D(y)}$$

$$D(x)= 1/n \sum_{i=0}^{n}(xi - E(x))$$

$$E(x)= 1/n1\sum_{i=0}^{n} xi$$

$$Cov(x,y) = 1/n\sum (x_i - E(x))(y_i- E(x))$$

Two or three indexes are used to calculate such a influence in the paper, viz., the number of pixel change rate (NPCR) and the unified average changing intensity (UACI), where:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\%,$$

$$UACI = \frac{1}{M \times N} \sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255} \times 100\%,$$

$$D(i,j) = \begin{cases} 0, & C_1(i,j) = C_2(i,j); \\ 1, & otherwise. \end{cases}$$

According to [30], the optimal values of NPCR and UACI are 98.61% and 32.46% respectively. Fig. 9 shows the results of NPCR and UACI with different iterations where quite a few iterations can make NPCR and UACI approach close to their optimal values. Fig. 9 shows that a pixel change in plain images can promptly cause a significant modified in the cipher image, too.

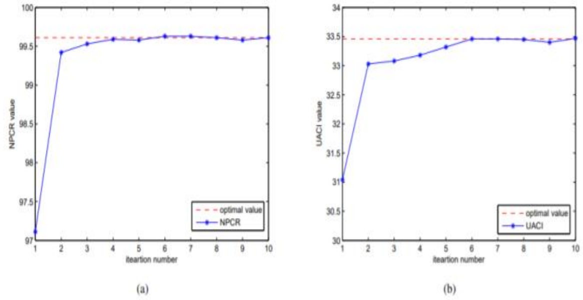


Figure 11: NPCR and UACI values at different encryption iterations.

C. BRUTE-FORCE ATTACK:

Brute-force attack or exhaustive attack is a basic method of trying every key values until the correct key is identified. Theoretically, the length of the key space determines the practical feasibility of performing a brute-force attack [7]. In our method, the generated key used to encrypt the compressed video in a frame is composed of a pseudo random binary sequence P R and an iteration number N. Let S contains set of all possible keys, |S| is the cardinality of S. The length of the binary sequence is decided by the size of the encrypted SVC block, which is set as 16 × 16. Since each columns in the 8X8 layered cellular automata transition rule, the same sequence denotes different rule sequences when different mapping function F is applied.

D. Layered Encryption Effects:

Taking the fate video sequence as a sample, we conducted a comparative experiment on the effect of layered encryption and decryption. As shown in Fig. 12, We statisticize a bitrate and peak signal-to-noise ratio (PSNR) of the video after decrypting the corresponding number of layers. The experimental results show that the bitrate and PSNR of the video increase with the number of decrypted layers, which means the quality of the video is improving. However, if only BL and EL2 are decrypted, the bitrate and PSNR are consistent with the BL layer, indicating that they have the same quality. That means the key of the Ith layer will not take effect until the I −1th is decrypted. So our proposed scheme can implement layered encryption and strict hierarchical control of SVC video.

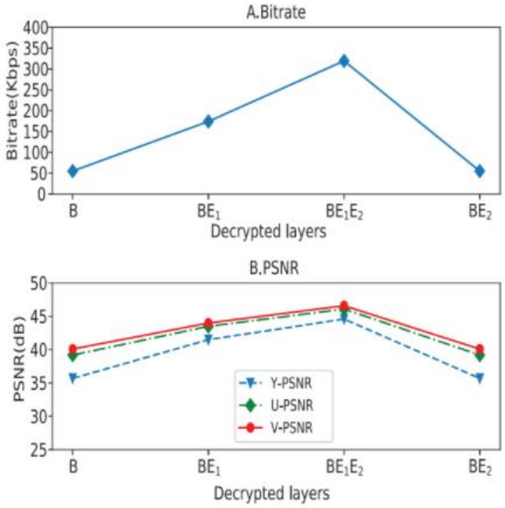


Figure:12
PNSR and bitrate after decrypting different layers.

IX.Conclusions

With the development of internet and cloud computing devices, the application of video surveillance systems have significantly increased in the last three decades because the explosive growth of multimedia computing, all the videos and data of surveillance stored in cloud computing or server only. In particular, the application of video broadcast system, video conference system and video surveillance system have put forward higher requirements on the security of video information. However, the early security methods rely heavily on access control, while their video information is not encrypted. Therefore, it is easy to steal the data during video transmission. Especially, if it is related to the military, economic and political sensitivity of the video data, studying the encryption of video data is more important.

Most well-known cryptographic algorithm are not suitable for surveillance video encryption due to the continuous use of surveillance video. A SVC encryption approach based on LCA is proposed. The SVCs are extracted from 8X8 layered column and then being encrypted by our approach and then stored in an cloud or at the camera's side[4], The admin can collect the original surveillance video with an on-demand manner. Since LCA is a highly parallel system, LCA-based encryption with the simple rules technique and shift transformations is inherently efficient and easy to be implemented. Finally, each SVC compressed video is divided into a set of binary blocks(8X8 layered columns) and all the blocks are encrypted simultaneously, the proposed method is applicable for the real-time requirements of surveillance videos. The experimental analysis show that our process satisfies both security and encryption algorithm requirements and is able to resist brute-force attacks as well as statistical attacks.

References

[1] XING ZHANG , SEUNG-HYUN "A Lightweight Encryption Method for Privacy Protection in Surveillance Videos" IBM Technical Report RC22886, 2017.

[2] Cheng Xu "A Hierarchical Encryption and Key Management Scheme for Layered Access Control on H.264/SVC Bitstream in the Internet of Things" IEEE INTERNET OF THINGS JOURNAL, VOL. 7, NO. 9, SEPTEMBER 2020

[3] G.Sai Vennela, N.Venkata Varun "PERFORMANCE ANALYSIS OF CRYPTOGRAPHIC ALGORITHMS FOR CLOUD SECURITY" 2nd International Conference on Inventive Communication and Computational Technologies – 2018

[4] ALBERT REGO , ALEJANDRO CANOVAS, "An Intelligent System for Video Surveillance in IoT Environments" IEEE INTERNET OF THINGS JOURNAL , date of publication June 18, 2018.

[5] D. A. Fidaleo, H.-A. Nguyen, M. Trivedi, "The networked sensor tapestry (NeST): a privacy enhanced software architecture for interactive analysis of data in video-sensor networks," Proc. of the ACM 2nd Int. Workshop on Video Surveillance & Sensor Networks, New York, NY, 2019.

[6] S. Moncrieff, S. Venkatesh, and G. West, "Dynamic privacy assessment in a smart house environment using multimodal sensing," ACM Trans. Multimedia Comput. Commun. Appl. vol. 5, no. 2, Nov. 2018, pp. 1-29.

[7] E. Newton, L. Sweeney, and B. Malin, "Preserving Privacy by De-identifying Facial Images," CarnegieMellon University, Technical Report CMU-CS-03-119, 2019

[8] P. Quintiliano, R. Guadagnin and A. Santa-Rosa, "Practical Procedures to Improve Face Recognition Based on Eigenfaces and Principal Component Analysis," Pattern Recognition and Image Analysis, vol. 11, no. 2, 2018, pp. 372-375

[9] Gonzalo Alvarez and Shujun Li, "Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems," International Journal of Bifurcation and Chaos, vol. 16, no. 8, pp. 2129-2151, 2019.

[10] X. Ma, W. K. Zeng, L. T. Yang, D. Zou, and H. Jin, "Lossless roi privacy protection of h.264/avc compressed surveillance videos," IEEE Transactions on Emerging Topics in Computing, vol. 4, no. 3, pp. 349– 362, 2016.