Volume 4, Issue 2, February 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

The IndexingAlgorithm for Scrambled Frames in Video Encryption

A. Shiva Krishna Reddy
Assistant Professor
Department of Information Technology
Sri Manakula Vinayagar Engineering College, India

K. Srimathi, R. Rajalakshmi
Department of Information Technology
Sri Manakula Vinayagar Engineering College, India

Abstract*— There are many algorithms in existence for scrambling of the video frames and to encrypt them. The proposed scheme treats the video as a framing sequence. The frames are sequenced by a provided algorithm. Secondly an index number is provided for each frame. Then the frames are encrypted to hide the information using thresholding method. Then the frames are sent in a random order. At the receiver side, the encrypted frames are decrypted. By using the index values the distributed frames are arranged again in a correct order. Proper keys are used to scramble the frames of the video initially. The content of the frames remains the same. The Grouping Of Pictures (GOP) provides a feature of categorizing the frames and pictures of same size under a particular group. This is provided to avoid blocking during transmission of video.

***Keywords*— scrambling video process; indexing; thresholding; rearranging**

I. INTRODUCTION

In the recent years video processing is lying at the peak of interest. Before transferring the video the process of encryption or compression is to implemented for security purpose. For the implementation of encryption discrete Fourier transform and message digest algorithm can be used. For the implementation of compression, techniques like wavelet transform and zero tree encoding are used. This reduces the size and hides the information. Video processing was introduced to encapsulate the information from the outside world. Many organizations consist of confidential data and it must be secured. Many of the existing systems of video processing are not applicable for the sensitive videos. Every second of video consist of frames. The frames are distributed into multiple frame sequences using a key. Then the frames are to be scrambled using another key. The entire contents are not hidden in this method. It is useful only for low sensitive videos. It is cost effective. The contents are always visible to the outside users. The cost of decryption will be greater than the original video.

In the existing system, the frames are just scrambled and sent through the network and rearranged at receiver side by using proper key. The receiver is not aware of the frame order. Since the existing system does not provides index value, the frames cannot be rearranged in the original order. Videos such as entertainment videos are of no use if they do not arrive in order. Video is efficient only if the frame sequence is met with the original video. The extension is provided by encrypting the entire content of the video. The threshold method is applied for the hiding of information. An index number is provided for each frame. Now the frame even when sent randomly can be rearranged at the receiver end with the help of index numbers. It can also be encrypted along with the frame.

II. RELATED WORKS

On the part of compression of video frames ‘n’ number of works has been developed. In the encryption phase the data carrying pixel should be hidden. We provide these to increase the secrecy of the data. In [1] compression efficiency and scrambling performance, decisions can be made about which elements should be encrypted at what compression efficiency loss. . In [2] three domains were used Intra-Prediction mode (IPM), residual data and motion vector difference values. Since three different domains were included for the base layer it is not efficient in terms of transmission. But the security is provided more by the encryption keys. In [3] DCT (discrete cosine transform) or DST (discrete sine transform) have been used. In this complete security is provided and the efficiency is maximum at this point. The disadvantage is that the actual output varies much with the predicted output. In [4] the frames are scrambled and then rearranged. All the information are not hidden. Only a part of information is hidden. The disadvantage lies with the rearrangement of the frames.

In [5] video encryption algorithm based on the DCT coefficients scrambling. The encryption algorithm is based on the concept of permutation group. Scrambling DCT coefficients of the permutation groups maintains the statistical property of DCT distribution so that the encryption does not suffer from DCT vulnerability attack. The disadvantage lies with the linearity of time complexity. In [6] the video is distributed across a peer to peer network. One to one communication is not efficient in the case of an distributed environment. The connection is needed to be established for a different destination. In [7] Watermarking has been integrated to avoid the requirement of separate keys for each spatial layer. The algorithm is better suited for multimedia streaming as the bitrate of the encrypted bitstream is lower than the original bitrate, but the system is not extended for protection of P and B frames.

In [8] the encryption of the video is provided by discrete cosine transform [DCT] which increases the scalability and confidentiality of the data. It consumes low resource. The disadvantage lies with the size of data. Compression is not provided and hence the time of transmission is more. In [9] the SSLFE and SMLFE algorithm have been used, it encrypts into single layer and multiple layer respectively. It provides security, compression overhead, error recovery. Both the algorithm provides negligible compression for the video. In [10] mix of linear transformation of coefficient values in DCT is used. But the quality of the video is degraded. In [11] fractal image compression algorithm and multiscale pyramid coding schemes is used. Hierarchy of bit-streams that can be used in multimedia applications. The quantitative evaluation of the algorithm is in the same range if not better than other published results for low-rate video coding.

III. EXISTING SYSTEM

The existing scheme represents an encryption method where the input video is distributed into multiple frame-sequences using a key and then these frame sequences are scrambled using another key to jumble the order of frames. These scrambled frame-sequences hold parts of video information and these parts are also not in the correct sequence. The scheme can be really useful for low sensitive videos where hiding of contents of each frame is not required. Till the completion of above explained steps the algorithm is very cost effective but the contents of individual frames are visible. As an optional extension, the scheme also proposes an algorithm for inter frame scrambling of pixels in these scrambled frame-sequences to degrade the individual frames.

This Inter frame scrambling significantly increases the computation cost, so it is required only when the contents of frames are sensitive. The scheme can be extremely useful for low sensitive videos like entertainment movie videos, as the cost of decrypting becomes higher than to buy the original video.

The advantages of the system are

- The System provides secured video transmission.
- Since the video frames are transmitted randomly it cannot be sniffed easily.
- The scheme provides an optional extension to degrade the visual quality of individual frames.

The disadvantages of the system are

- Increased computational cost.
- Each frame is compared with previous frame which results in time complexity.
- Rearrangement is difficult since the frames are sent in random.

IV. SYSTEM ARCHITECTURE

The system architecture or the design gives value of revealing the process that is done during the experimental works. The sender first authenticates himself to enter the system which is known as the login details that stored in the database. Then he takes the video that he wants to transmit and collects the data that are important in that video and then encrypts the video by breaking the video in frames and further in pixels.

The video is broken into frames by sequencing algorithm. Then an index number is provided for every frame in the video. The encryption is done. this encrypted video frame will be transmitted over the networks and it will be reconstructed as frames in the receiver end. Then the original secret data is said to be constructed and then the original video can be regained. The frames are sent in random. If the frames are sent in the same sequence it is easy for a hacker to get through the information. The reconstruction of the frames is associated with multiple strategies. The receiver should initially decrypt the frames. Then by the provided index numbers, the frames are arranged in the order. Since the frames are sent in random, we require an algorithm to re arrange. By using the index numbers, the frames are arranged and a full fledged video is obtained to the receiver. The video is of no use if it is not in a proper sequence. On looking at entertainment videos, the order of the frames plays a vital role.

In fig.1 it is clearly shown that the sender follows file selection, indexing and scrambling of the frames. Encryption is also done at that point which hides the information entirely and transmits as binary frames to the receiver. Whereas the receiver follows procedure to obtain the original video that has been transmitted by the sender with the help of secret key. The secret key is known only to the sender and this increases the confidentiality of the transmission process.

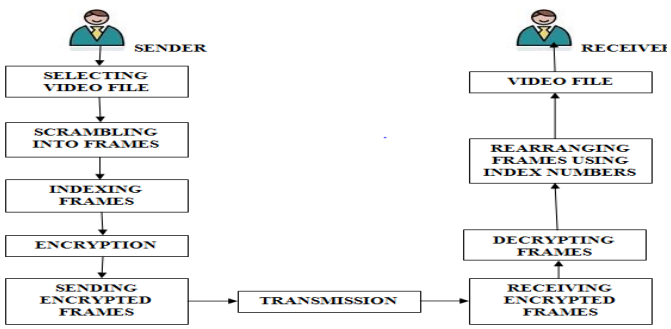

Fig.1 System Architecture Design

V. PROPOSED WORK

Every frame of a video is encrypted. Then the encrypted frames are given an index number. The index number is also masked. The encrypted frames are scrambled and sent through the network in a random manner. Completely all the information is hidden. The threshold method is used for encrypting the frames. The threshold method converts the data into a binary data. The threshold value is identified. The repeating pixel value is taken as a threshold value. The pixels greater than or equal to the threshold is taken as 1, and the values lesser than the threshold value is taken as 0.The receiver is provided with the decrypting algorithm. The original frames are obtained and rearranged with the help of index numbers.

Scrambling into Frames

The proposed scheme distributes the video into n number of frame sequence. A distribution key is provided. With the help of distribution key the location for the frame is obtained. N denotes the frame sequence. In this algorithm the entire video is said to be broken into input frames then the encryption is said to be done only in the part that has changes in it. The total frames that is said to be present is represented as NumOfFrames, the value Input Frame[h] represents the total input that is said to be present in the video

Fseqi represents that the sequence in which the scrambling process take places. Distribution key[h] is said to the secret code that is sent to the receiver for decrypting the data for regaining the original data. The value examine[h] in figure represents how the frames are gathered and noticed to indentify the changes in the video and scrambling it for the purpose of encryption. Hence the value before scrambling is said to be known as the examine [h]. n sequence represents that how the frames are said to formed after scrambling.

The value of 'a' is incremented after every frame to shift over to the next frame. Once the entire video is sequenced the process ends. It begins with the indexing as per the option from sender.

The value examine[h] in figure represents how the frames are gathered and noticed to indentify the changes in the video and scrambling it for the purpose of encryption. Hence the value before scrambling is said to be known as the examine[h]. 'n' sequence represents that how the frames are said to formed after scrambling.

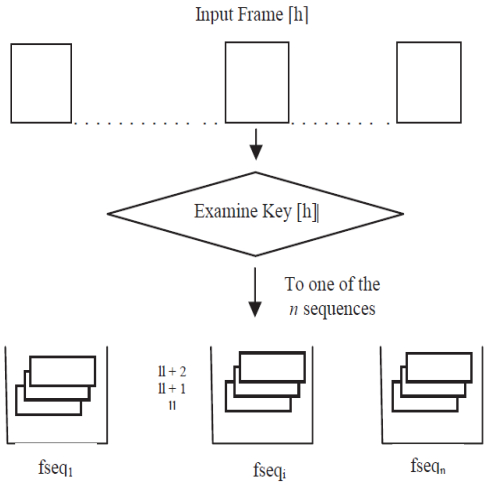

Fig. 1 scrambling of video frames

Algorithm 1

```
a= 1;
for h = 1:NumOfFrames
  Examine (distribution key[h]) and  find i
            Fseqi[a] = Inputframe[h];
           a= a + 1;
         end
end for
```

Indexing Frames

An index value is generated for each frame. The value lies in the order by which the frames can build a video. The index numbers can also be hidden for the purpose of high confidentiality. As soon as the frames are sequenced the index number is provided. Then the data values are hidden by using the step 3.

x= (w-tw)/2:
*y= h-(2*lh)-n:*

Hiding The Information

The equations are an exception to the prescribed specifications of this template. You will need to determine whether or not your equation should be typed using either the Times New Roman or the Symbol font (please no other font). To create multileveled equations, it may be necessary to treat the equation as a graphic and insert it into the text after your

paper is styled. The thresholding method plays a vital role in hiding the information. The maximum repeated value in a particular frame is assumed to be the threshold value (T). It varies for every frame. The values greater than the threshold values or equal to the threshold values are taken as 1. The values lesser than the threshold values are taken as 0. Now an entirely encrypted binary frame can be obtained which hides the information. Algorithm 2 is used to encrypt the frame. The action for reversing is obtained with the help of public key which is sent to the receiver side and it is not known to the outside world. The reverse action provided in algorithm 3 is used to decrypt the frame.

Algorithm 2

⟨Threshold(T,M)⟩ ≡

```
For each Pixel in frame
    if (Pixel >=T)
    then    replace[Pixel] = M
    else
            replace[Pixel] = 0
```

The algorithm for hiding of information reveals the process of protecting the information for the unauthorized network. The term for each pixel in frame gives the meaning that a value is said to be assigned for the each pixels divided in the frame. The threshold value is said to be assigned determined by viewing that which pixel in the frame is repeated maximum. Replace [pixel] is the term that determines when the value of the pixel is to lesser than threshold value then it is assigned as 0. When the value of pixel is greater than it is assigned a value zero. T determines whether the value of pixel is greater or lesser than the threshold value. When the value of the pixel is greater than the threshold value then M is assigned as one.

Example:

7	6	5	7	8	5	4	1
7	7	5	7	4	3	1	6
3	2	6	8	9	7	5	7
9	7	5	3	2	1	9	7
5	7	4	1	7	8	0	7
7	3	4	7	5	7	8	2
7	2	7	3	7	5	7	7
3	7	7	2	7	6	1	0

Fig 3: Before Applying threshold to a frame

T=7

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

Fig 4: After Applying threshold to a frame

VI. CONCLUSION

This paper concludes an efficient algorithm for encryption and compression of scrambling video process. Since the existing works are not that much good in the encryption so this paper gives and better one. In this paper we are proposing an encryption for the multimedia application especially in video transmission over the communication networks. Here in this paper the process encryption is been given a detailed explanations for the videos in two dimensional process. Hence this paper can be future enhanced for the purpose encrypting the video in the three dimensional one.

ACKNOWLEDGMENT

We would like to express my special thanks of gratitude to Mr.A.Shiva Krishna Reddy who gave guidance as well as Mr.R.Raju Head Of Department who gave me the golden opportunity to do this wonderful project on the topic Scrambling and Indexing Of video Frames, which also helped in doing a lot of Research and I came to know about so many new things I am really thankful to them. We would like to thank Dr.G.Shanmuga Sundaram for numerous suggestions and modifications to improve the presentation and readability of this paper.

REFERENCES

[1] Glenn Van Wallendael, Student Member, IEEE, Andras Boho, Jan De Cock, Member, IEEE, Adrian Munteanu, Member, IEEE, Rik Van de Walle, Member, IEEE "Encryption for High Efficiency Video Coding with Video Adaptation Capabilities", IEEE Transactions on Consumer Electronics, Vol. 59, No. 3, August 2013.

[2] L.M.Varlakshmi, G.Florence Sudha, G.Jaikishan,"An Efficient Scalable Video Encryption Scheme for Real time applications" International Conference on Communication Technology and System Design, Procedia Engineering vol 30 (2012) 852 – 860.

[3] Siu-Kei Au Yeung, Student Member, IEEE, Shuyuan Zhu, Member, IEEE, and Bing Zeng, Member, IEEE "Design of New Unitary Transforms for Perceptual Video" Encryption IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 21, NO. 9, SEPTEMBER 2011.

[4] Jitendra Rajpurohit, Dr. Ajay Khunteta "A Scalable Frame Scrambling Algorithm for Video Encryption" IEEE Conference on Information and Communication Technologies.

[5] Hao Wang and Chong-wei Xu, "A new lightweight and scalable encryption algorithm for streaming video over wireless Networks".

[6] Andras Boho, Glenn Van Wallendael, Ann Dooms, Jan De Cock, Geert Braeckman,Peter Schelkens, Bart Preneel, and Rik Van de Walle,"End-To-End Security for Video Distribution" signal processing in the encrypted domain.

[7] Zafar Shahid, Marc Chaumont and William Puech," selective and scalable encryption of enhancement layers for dyadic scalable h.264/avc by scrambling of scan patterns", "ICIP'09: International Conference on Image Processing, Cairo, Egypt"

[8] Hao Wang and Chong-wei Xu," A new lightweight d scalable encryption algorithm for streaming video over wireless Networks" Computer Science and Information Systems Kennesaw State University.

[9] Bin B. Zhu, Senior Member, IEEE, Chun Yuan, Yidong Wang, and Shipeng Li, Member, IEEE, "Scalable Protection for MPEG-4 Fine Granularity Scalability" IEEE TRANSACTIONS ON MULTIMEDIA, VOL. 7, NO. 2, APRIL 2005.

[10] YuanZhi Zou, Wen Gao "A novel algorithm of spatial scalability for scrambled video" 0-7803-8834-8/05/$20.00 ©2005 IEEE.

[11] Alexandru Bogdan, "Multiscale (inter/intra-frame) fractal video coding" Proceedings of the IEEE Conf. ICIP-94.

