A RANDOMIZED SELECTIVE ENCRYPTION USING HASHING TECHNIQUE FOR SECURING VIDEO STREAMS

Lizyflorance. C[1], Lalitha Kumari. R[1]
School of Information Technology and Engineering,
VIT University,
Vellore-632014, India.

Prof. John Singh K[2],
Assistant Professor (Selection Grade)
School of Information Technology and Engineering,
VIT University,
Vellore-632014, India.

Abstract - **Digital video transmissions are widely used in network nowadays. Hence, securing its contents and keeping privacy is vital. Several encryption algorithms have been proposed earlier to achieve secure video transmission. But altogether attaining efficiency, security and flexibility is a major challenge. To transmit a digital video, encryption is necessary to protect its contents from attacks. As the size of the videos are usually large their contents has to be compressed before transmission. Encryption is applied on the video content after compression. One of the encryption technique selective encryption is used for encrypting video. It encrypts only a subset of data. The selective encryption algorithm reduces the amount of the data to be encrypted and achieves a required level of security. In this paper we study the existing selective encryption algorithm and its classifications. The challenges in the selective encryption algorithms and some future directions are presented.**

Keyword: Frame slicing, I-frames, MD5, Macro Block, Selective Encryption.

I. INTRODUCTION

Selective encryption is an encryption technique applied on video data in which some subsets of the data are encrypted to reduce the encryption overhead. Selective encryption at the source end select frames of the input video. The video frames are classified as I-frame, P-frame and B-frame [1]. Frames are selected and encryption techniques are applied on the selected frames to achieve visually degraded effect. The encrypted video is transmitted over the network to the destination. At the destination the encrypted video obtained is sent to a decryption block. The decryption block decrypts the video frames that are encrypted and a quality video is given as output. Many selective encryption algorithms have been proposed and improved in the recent years. Each algorithm differs from each other. The objective of the selective encryption is to reduce the computational workload and processing time and to attain the required security level [6]. Even though the selective encryption focuses on securing video it does not consider the optimal delivery of video frames in the erroneous wireless transmission. The major research now in selective encryption is to encrypt which part of the video data to achieve visually degraded effect. In this paper the challenges in the selective encryption algorithms are discussed and data's are selected randomly and encrypted to achieve efficiency.

II. EXISTING SYSTEM

Yuefa Hu, Xingjun Wang have proposed a paper[1] that deals with encrypting the data with different ratio levels to attain highly secured level of encryption and to achieve visually degraded effect. The selective encryption is done on different selected data with different type of algorithms in accordance with the selected factor to achieve better encryption. The following steps are followed to encrypt the data. For every 100^{th} macro block encryption is done and replaced by the values possible in accordance with type of frame. According to the type of frame whether it is I- or P- frame select the slice header and calculate the amount of each slice. Amount of all slices for the data has been compared and its positions are remembered for the slices having large amount of data. Five slices which has large amount of data have to be selected to encrypt if the frame belongs to I-frame. Two slices which has large amount of data to encrypt has to be selected if the frame comes under P-frame. The slice whose macro block is encrypted should not be taken for encryption. Other than that slice, the slice has the large amount of data is considered for encryption. Using AES algorithm every first macro block of selected slice will be encrypted. The above steps are repeated for each and every frame. The improvement in

this type of encryption is greater to achieve a visually degraded effect because the ratios are fixed differently according to the importance of data.

PremKumar.T and Prakash.V.R has proposed advanced UEP (Unequal Error Protection) and selective encryption [2] for video in wireless sensor networks. During block based encryption the error in bits occur due to extra dependency bits in the encrypted blocks. This will cause packet loss during transmission and in media decoding misrepresentation will occur during video frame transmission. To provide better quality in multimedia service UEP based network resource allocation algorithm is used. To find the optimal allocation method for I, B and P frames the cross-layer resource allocation approach in used. As the key length in the encryption block increases the dependency involved in encryption increases. To provide high quality service for wireless sensor networks in multimedia environment the bit padding is done at the application layer during encryption. There is also a chance for decoding latency as the multiple frames belongs to encrypted codeword. The decoding of video frames depends on the arrival of encryption block. The encryption blocks of smaller size reduce the decoding latency. The next stage for the proposed algorithm is it to make an analysis on complete frame level decoding dependency to allocate the priority among the video frames. While considering the video frames which are compressed, the I-frame is independent of any video frame whereas decoding the p-frame entirely depends on the previously decoded I-frame and the B-frame depends on both I and P frames. In this algorithm the budget for encrypted bit is limited so the priority must be analyzed well to be used in a limited way. As a result of this algorithm the video frames are sorted according to the frames which are important for other succeeding frames of the current video frame. As a result of this UEP based network utilization the gain in performance is based on comparing the distortion-encryption with the previous existing encryption algorithms on video streaming. In this paper the energy efficiency is also considered as one of the major factor in wireless sensor networks apart from the quality of video transmission.

Adnan M.Alattar, Ghassa I. Al-Regib and saud A. Al-Semari have proposed a paper [3] to reduce the processing time by preserving the security. Three methods have been proposed in this paper with three different approaches as follows: In Encrypting Intra-Coded Macro blocks alternatively the data of n^{th} I-macro block is encrypted and the rest I-macro blocks are not considered. This method is also called as Method I. Each and every I-macro block is encrypted by using the counter which keeps track of the macro blocks and it is updated in the beginning of each slice. Some of the blocks are left unencrypted and this is due to differential coding scheme. The processing time is less when compared to the encryption done on all I-macro blocks. In this the I-macro blocks are encrypted alternatively and the headers of all the predicted macro blocks are encrypted to improve the security level of the Method I every header including the I-macro block are encrypted using DES algorithm. DES algorithm works on 64-bit segment and it starts from header of each predicted block. The segment may include part of the header or of the entire header. If the segment which is encrypted includes the part of the header it causes the synchronization problem but it increases the security of the video transmission. In I-Macro blocks and the headers of predicted Macro blocks the encryption is done on every I-macro block and every predicted nth macro block header. To perform this action two counters are used to keep track of the header of predicted macro block and encrypted I-macro block. DES algorithm is used for encrypting macro block and also the header.

Seohyun Jeong, Eunji Lee, Sungju Lee, Youngwha Chung have proposed a paper [4] about slice-level selective encryption algorithm to achieve reduced computational workload compare to SECMPEG around 30%. In SECMPEG whole I-frames are encrypted where I-frame size is larger when compared to B and P frames. In slice-level encryption, only first data in each slice is encrypted. The effect of encryption is attained in most of the I-frames and it develops an error propagation property in MPEG2 standard. In general MPEG video is done on duplication of group of pictures (GOPs). Each GOP is of I-, P-, B- frames which are selected in sequence. I-frames are encoded as standard JPEG, where P- or B- frame are encoded for the difference between close frames based on motion compensation. When motion compensation cannot find matching block in close frames, the macro blocks associated with it are encoded as intra-coded mode and is called as I-block. This I-block contains the large amount of motion in P- or B- frames which are encoded as standard JPEGs. Encrypting the whole data is tedious. For providing proper level of security and to reduce the computational workload SECMPEG encrypts I-frame and I-block selectively. And it also provides 5 security levels. In those levels of security, level 3 encrypts I-frame whose size is larger than P- and B- frames. In addition 30% data is needed for encryption in mobile phones without the reduction in security level. In slice level encryption of videos if the attacker after Compressing/encoding process distorts the first macro block in each slice that block is inconsistent with the header data. If the attacker tries to decode the distorted macro block with the correct header data, it propagates the error to the successive macro blocks in the slice. In this algorithm the attacker who does not have the key needs to decode/decompress the data which is transmitted to view the video.

S.no	Type of frame selected	Encryption Algorithm	Encrypted Content of Data	Advantages
1.	Macro block of P-frame, I-frame and I-block[1]	AES(Advanced Encryption Standard)	Every 100^{th} macro block is encrypted. Sliced I frames of large amount of data.	High security level
2.	I-,B-,P- frames[2]	UEP(Unequal Error Protection)	Video frames are sorted according to their weights and encryption is done based on the dependencies of the current video frame	Improves Energy Efficiency and Robustness
3.	I-macro block[3]	DES(Data Encryption Standard)	Method-1: Alternatively encrypts the macro block. Method-2: Alternatively encrypts I-macro block and headers of all predicted macro block. Method-3: Encrypts n^{th} I- macro block and headers of every n^{th} predicted macro block	Reduces the processing time.
4.	I-frame [4]	Slice-level selective encryption	Encrypts first data in each slice and the effect is propagated throughout the slice.	Less computational workload.

TABLE 1: Classification of Selective Encryption

III. RECENT ISSUES IN THE EXISTING SYSTEM

From Table 1 the above proposed algorithms have one or more of the following problems that gives a negative impact on selective encryption. Even though these algorithms provides confidentiality of video data it does not ensures authenticity. It results in insufficient security.Increased key length results in complexity and increases encryption overhead. The key size should not exceed the commonly used key size in modern ciphers. The AES and DES algorithm follows symmetric key encryption. As the symmetric key encryption has increased key length it decreases the compression efficiency.

IV. PROPOSED SYSTEM

Our proposed work is to selectively encrypt the data. The video can be divided into macro blocks. Using a random number select macro block and encrypt the selected macro block using hash based encryption. Videos are classified into frames as I-frame, B-frame and P-frame.

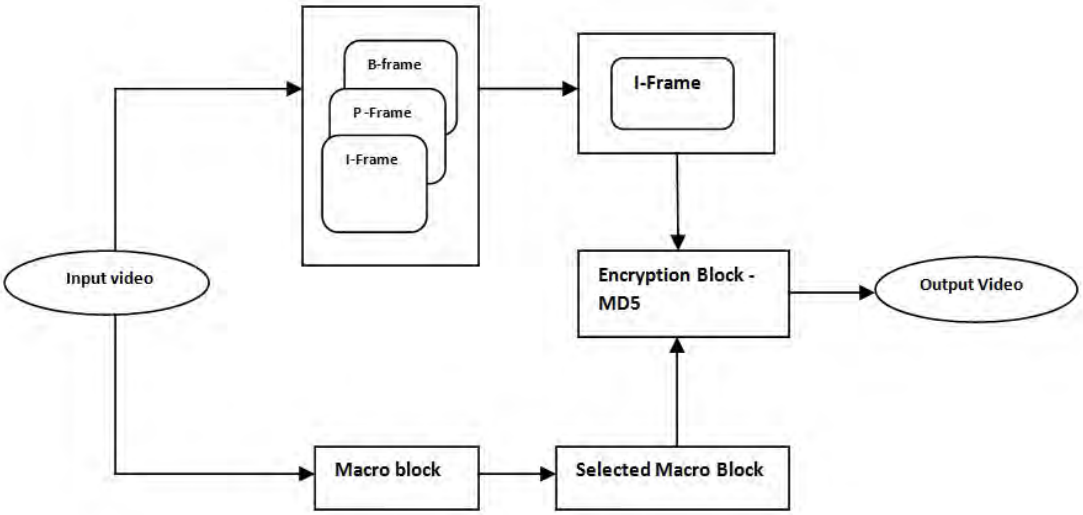

Fig.1.1 Architecture Diagram of Proposed System

I-frames are selected and sliced. In the sliced data the slices that contain the large amount of data are to be selected. Along with the macro block the sliced I frames also encrypted using hash based encryption.

As in the Fig.1.1 our selective encryption has the following steps

1. Macro blocks are selected randomly using random number. The selected macro blocks are sent to the encryption block.
2. The encryption block consists of the MD5 hash encryption code.
3. A video can be divided into three types of pictures in MPEG namely the I-Frame, P-frame and the B-Frame.
4. Select I-Frames and slice the I-Frame. From the sliced I-Frame select slice that has large amount of data and send it to the encryption block. If the encrypted macro block is in the sliced I-frame do not consider it for encryption.
5. Repeat the steps until a desired visually degraded video is obtained as output.

V. SECURITY ANALYSIS

5.1 Statistical attacks

Statistical attack is based on predictability. Predicting the relationship between the data and the encrypted data may allow an attacker to determine the plain text without decryption. But our proposed schema is encrypted until our desired visually degraded video is obtained as output. And also the bits are transformed in fixed length format. So the attacker can hardly predict the frame.

5.2 System use attacks

System use attack is based on the encryption system used. The encryption system used should increase the security. Instead of the symmetric and asymmetric key ciphers [5] hash based ciphers are used. The MD5 algorithm converts the bits into fixed length format regardless of the size of input. So it is hard to predict the encrypted frame. Encryption is done on macro blocks as well as on the sliced I-frames. It can greatly improve the security level and reduces the computational overhead.

5.3 Perceptual attacks

This attack is due to the perceptual redundancy. A successful attack is the intruder may be able to predict the visual as well as the audible information even though the portion of the bit stream is damaged without the decryption key. But in the proposed scheme the selective data is keep on encrypted. It is hard to perceive the encrypted data.

Our future work is to work on audio for increased security and to work on the security attacks still persisting. As a technology increases we must also be in a position to adapt changes and to achieve video encryption with greater extent.

VI. IMPROVEMENTS

Our Algorithm greatly reduces the rate of encryption as it selectively encrypts the data. The most important data in the I-frames and the randomized macro blocks are taken into account for encryption. The MD5 hashing encryption is used to achieve visually degraded effect with less computational workload without generating key it transforms the message into fixed formats. This fixed format of 128 bits avoids collision as much as possible

VII. CONCLUSION

Selective encryption is a part of encrypting subsets of video data. We presented a survey about the existing selective encryption algorithms, their issues and the future detections. The main research in selective encryption algorithm is to propose secure schemes that are error resistant, energy efficient, less computational overhead, high security and also it reduces the amount of data to be encrypted while achieving a desired level of security [7]. The hash based encryption algorithms are applied on selective data to reduce computational overhead with desired level of security. It avoids collision as much as possible. Still this algorithm can be improved better by working on robustness and increased visually degraded encrypted video. In the above selective encryption algorithms surveyed the key generation is not handled properly. Developing an algorithm with increased robustness is a challenging issue. Algorithms should be energy efficient, reduce encryption dependency overhead and process time. Security and storage requirements have to be discussed in depth in the upcoming proposals.

VIII. REFERENCES

[1] Yuefa Hu, Xingjun Wang, "*A novel selective encryption algorithm of MPEG-2 streams*",on IEEE 2012, Article ID 978-1-4577-1415-3/12,pp 2315-2318.

[2] PremKumar.T and Prakash.V.R, "*Advanced UEP and selective encryption based video streaming in Wireless Sensor Networks*", International Conference on computing and control engineering (ICCCE 2012) 12 & 13 April,pp 1-8.

[3] Adnan M.Alattar, Ghassa I. Al-Regib and saud A. Al-Semari, "*A two-way selective encryption algorithm for MPEG Video*".

[4] Seohyun Jeong, Eunji Lee, Sungju Lee, Youngwha Chung,"*Slice-Level selective encryption for protecting video data*", International conference on Information networking(ICOIN),pp.54-57,2011

[5] M.Abomhara, Omara Zakaria, Othman O.Khalifa, "*An Overview of Video Encryption Techniques*", International Journal of Computer Theory and Engineering, *Vol.2*, pp. 103-110,No.1 February, 2010

[6] Fuwem Liu, Hartmut Koenig, "*A survey of Video encryption algorithms*",Computers and Security 29(2010) pp. 3-15.

[7] A.Massoudi, F.Lefebvre, C.De Vleeschouwer, B.Macq, and J.-J. Quisquater**,** "*Overview on Selective Encryption of Image and Video: Challenges and Perspectives*", Hindawi Publications Corporation EURASIP Journal on Information Security, *Vol. 2008*, pp 1-18, Article ID 179290.