Scientific Journal Impact Factor (SJIF): 1.711

International Journal of Modern Trends in Engineering and Research

ISSN (ONLINE) : 2349 - 9745 ISSN (PRINT) : 2393 - 8161

A New Security Primitive For Authentication And Data Transfer

Naveena Jose[1], Geethu Mohandas[2]

[1]*PG Scholar,* [2] *Asst.Professor*

[1,2]*Department of Computer Science Engineering,*

Indira Gandhi Institute of Engineering& Technology Nellikkuzhi, India

Abstract—The data transfer become the most part of our daily life. Data may be like images, videos, files etc. When we send multimedia content, it need to be encrypt and compress for the security of the data. Many hacking and misuse of data will happened during it send through the internet. Most of the existing system will adapt the compression then encryption system. This paper is based on the encryption then compression method. Also apply the permutation operation to the data. The clustering and random permutation are already exists in the image. Through this paper we extend it to the videos. Where each frame will be considered as the images By adapting this method the data security will be increased.

Keywords—Encryption Then Compression (ETC), Permutation, Cryptography

I. INTRODUCTION

Millions of groups are using online services for different daily activities, many of which require giving out personal information with the service provider. People use social networks to get in contact with other people, and generate and share content that includes personal information, images, and videos. The service providers have right to the content provided by their users and have the right to process collected data and distribute them.

The area of information technology increasing day by day. By the use of this internet the data transfer from one place to another became easy and fast. Every information from sender to receiver can be send within a minute through the internet without considering the geographical and other circumstances. Same way the chance of data misuse also increased. Every user will focus on the security of their data.

Present systems offering efficient and safe communication. But it failed to data transfer through a secure channel. Most of the existing system will focused through the compression the encryption system. Complication may arise when the encryption and compression are not performed in well manner. So the sender and receiver will take care of the data operations. In this paper uses the encryption then compression method. Proposed image encryption algorithm is performed over the domain of the mapped prediction error. In this method firstly construct a prediction error domain based on this input data. By comparing the original and predicted error, obtained a prediction error image. After that the permutation, encryption and compression will be applied to this predicted error image. For this time a user defined key will be generate to the security of data. The prediction error obtaining based on the algorithm Context-based, Adaptive, Lossless Image Coding(CALIC).It obtains higher lossless compression of continuous tone images than other techniques. By this paper this extend the image clustering and operation to the video data.

The rest of this paper is organized as follows. Section II gives the details of related work of ETC system, where image operations is considered. Extension to the case of video is given in Section III. We conclude in Section VI.

II . RELATED WORKS

Addition to the theoretical analysis, Johnson et al. [5] propose a practical approach to the lossless compression of encrypted black and white images. In this paper we consider the extension of the work in to the case of lossless compression video of grey level. The opportunity of processing encrypted signals directly in the encrypted domain has been receiving increasing attention in recent years [3]. In addition to the theoretical findings, [5] also proposed practical algorithms to losslessly compress the encrypted binary images. Schonberg et. al later investigated the problem of compressing encrypted images when the underlying source statistics is unknown and the sources have memory [3]. By applying LDPC codes in various bit-planes and exploiting the inter/intra correlation, Lazzeretti and Barni presented several methods for lossless compression performance on the encrypted grayscale/color images [12].By the existing system operated based on the figure (a).Based on this method it have small security. Because the encryption take only after the compression.

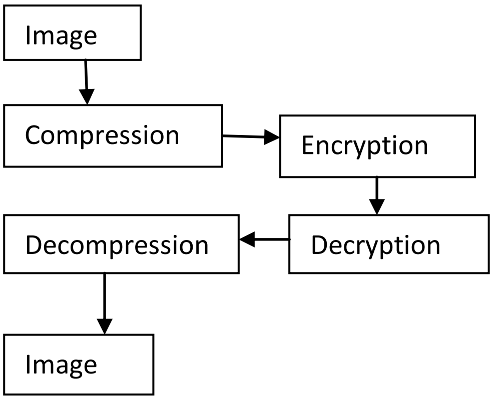


Figure (a):CTE System

From the above figure ,it shows that the compression encryption method. Most of the existing system are based on this method. One problem for using this method, it cause the loss of efficiency of data. The image compression is mainly lossy and losseles image compression. So when selecting the algorithm, It should be losseles. Because when sending an image from one user to another the data must be accurate.

The image and video data gathered and video sharing sites, street view, surveillance cameras and institutional databases can easily be used by autonomous systems that use efficient face detection and recognition algorithms to identify and track individuals. This capability raises serious privacy concerns among people. As a result of these concerns, we have witnessed a significant increase in the number of privacy related research in the field of the image and video data in recent years. In the following, it briefly summarize the state-of-the-art that uses cryptographic techniques to address the privacy issues in the field of image and video processing.

Senior and Pankanti provide a details of privacy and give a brief conclusion on the privacy protection mechanisms for face recognition systems. Lu discuss problems and challenges in secure video processing. The solutions based on cryptographic techniques proposed in the literature focus on different techniques like homomorphic encryption (HE), secret sharing and multiparty computation. Avidan and Butman propose a face detection algorithm based on machine learning that is particularly designed for realizing the algorithm efficiently by using secure multiparty computation. Erkin propose to encrypt face images using HE and let the Eigenface recognition algorithm work on encrypted data without revealing private information to the holder of the face database Sadeghi further improve the efficiency of that approach by replacing the matching mechanism with a fine-tuned garbled circuit

III. PROPOSED WORK

The proposed method based on the video data. All the operation in the images are extended to the videos. This use the Encryption Then Compression (ETC).Based on this, first data encrypted and then compressed. This shows in the figure (b).

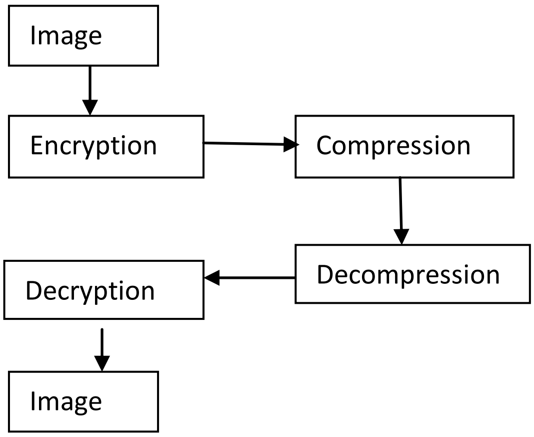
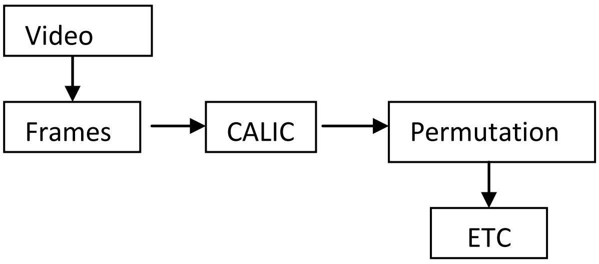


Figure (b): ETC System

The chance of processing encrypted signals straightly in the encrypted domain has been receiving increasing attention in recent years. From the whole ETC system, the design of the encryption algorithm should simultaneously consider the security and the ease of compressing the encrypted data. To this end, this propose a video encryption scheme operated over the prediction error domain. For the prediction error domain, use the CALIC algorithm.

In video, it will contain number of frames. Apply all the operation in this frames. Each frame considered as the images. So firstly the user need to load the video. And after that should specify the number of frames need to be processed. Based on this number of frames the prediction error domain start the operation. For this here it apply the CALIC algorithm. Based on this algorithm first it make raster scan on the image I. Here each pixel should be anlaysed. After that context based prediction take place in each pixels in the image I. It can represented as I^. And for the prediction error image it need to compare the original image and context based prediction error image. When comparing this image the output error image obtained is termed as e. That means the prediction error e is the difference of original and context based prediction error image, e=I-I^. The proposed system idea shown in the figure (c).It explain the sender side operation.



Figure(c): Proposed System of Sender

From this it shows that first it load the video. And after it specify the number of frames. In the specified number of frames the CALIC algorithm will be applied. Then in that processed frame it need to apply the random permutation. Permutation can be obtained by the raw shift and column shift. So for this user enter a key to specify the number of times that the row and column to need shift. And this same key should need to pass the receiver side. The mismatch in the sender and receiver side key do not provide the accurate data. After the permutation it need to ETC operation. So the permuted data to encrypt based on the keys. Then it compressed.

In the receiver side it firstly accept the compressed data. So it first need to be decompressed. After the decompression the data in the encrypted format. Based on the sender side key it then decrypted. If the keys are different then proper decryption can't be take place. Then apply the depermutation to the decrypted image. By the permutation provide more security to the system. So here used the permutation. After all this it get as the original images. And make it to the frames. So finally the receiver can effectively retrieve the actual data. By the use of CALIC algorithm it can be applied to the lossy and losseless images. All the operation in the sender is reversed in the receiver side. proposed image encryption algorithm is performed over the domain of the mapped prediction error e. Instead of processing all the prediction errors as a whole, this separate the prediction errors into clusters based on a context-adaptive approach. The successive randomization and compression need to be benefited from this clustering operation. So it help to apply the similar operation in a group and also save the processing time.

In the case of the image only operation it the faster in the operation. But in the video when the number of frames increased operation and processing time also increase. Because in video it process the multiple number of images at a time. Here the user have the freedom to specify the number of frames that want to process. Otherwise it can be automatically processed the full video. By the easy and efficient algorithm it provide more security to the data. Within the proposed system, the video encryption has been achieved via prediction error clustering and random permutation. Highly efficient compression of the encrypted data has then been realized by a context-adaptive arithmetic coding approach. Compared with the traditional predictive coding system in which the compression is conducted over the original, unpermuted prediction error sequences.

By analayzing our proposed method it seem to more efficient than the existing method. Because more security operation like ETC, permutations are applied in the proposed method. The aim of a user is to send his data with maximum security. Here it provide both type of data as image and video. The basic concept is from the image and this paper extended this into videos. Encryption to compression applied in this paper have the great important part.it can use both lossy and lossles image compression. But mainly this focus to the lossles image compression. Noise in the image can also be considered in this process. Ultimate aim in this paper is to provide the maximum data security to the user when they send data from one user to another one. Because through the internet the possibility of hacking and misuse of data is high. So it need to avoid. For this different operation can be performed in the data. So the hacker can't be easily attack the valid data.

IV. CONCLUSION

Encryption and compression are the important part of image processing. This will be improve the security of the data. Through this paper it can see that the video encryption through the random clustering. In here it processed each frames in the video. And each of this frame considered as the different images. And apply the encryption, compression and permutation to this images. And receiver side the reverse process take place and the frames are combined and form the video again. One of the limition in this case is when frame number increase the processing time also increasing. It can be solve on the future work

REFERENCES

[1] J. Zhou, X. Liu, and O. C. Au, "On the design of an efficient encryption then- compression system," in Proc. ICASSP, 2013, pp. 2872–2876.

[2] M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, "On compressing encrypted data," IEEE Trans. Signal Process., vol. 52, no. 10, pp. 2992–3006, Oct. 2004.

[3] D. Schonberg, S. C. Draper, and K. Ramchandran, "On compression of encrypted images," in Proc. IEEE Int. Conf. Image Process., Oct. 2006, pp. 269–272.

[4] D. Klinc, C. Hazay, A. Jagmohan, H. Krawczyk, and T. Rabin, "On compression of data encrypted with block ciphers," IEEE Trans. Inf. Theory, vol. 58, no. 11, pp. 6989–7001, Nov. 2012.

[5] M. Johnson, P. Ishwar, V. Prabhakaran, D. Schonbergand K. Ramchandran, "On Compressing EncryptedData" IEEE Tranaction on Signal Processing vol.52no.10 pp. 2992¡3006, October 2004.

[6] X. Zhang, G. Feng, Y. Ren, and Z. Qian, "Scalable coding of encrypted images," IEEE Trans. Imag. Process., vol. 21, no. 6, pp. 3108–3114, Jun. 2012.

[7] W. Liu, W. J. Zeng, L. Dong, and Q. M. Yao, "Efficient compression of encrypted grayscale images," IEEE Trans. Imag. Process., vol. 19, no. 4, pp. 1097–1102, Apr. 2010

[8] X. Zhang, G. Sun, L. Shen, and C. Qin, "Compression of encrypted images with multilayer decomposition," Multimed. Tools Appl., vol. 78, no. 3, pp. 1–13, Feb. 2013.

[9] X. Wu and N. Memon, "Context-based, adaptive, lossless image codec," IEEE Trans. Commun., vol. 45, no. 4, pp. 437–444, Apr. 1997.

[10] M. J. Weinberger, G. Seroussi, and G. Sapiro, "The LOCO-I lossless image compression algorithm: Principles and standardization into JPEG-LS," IEEE Trans. Imag. Process., vol. 9, no. 8, pp. 1309–1324, Aug. 2000