International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 3 276 - 277

Video frame data conversion of the RGB feature sequence

Mr. A. Ragavan
M.Tech Assistant professor
Department of Information Technology
Skp engineering college
Thiruvannamalai, Tamilnadu, India.
E-mail- Athiragav@gmail.com

D. Revathipriya
Department of Information Technology
Skp engineering college
Thiruvannamalai, Tamilnadu, India.
Email- revapriyaitb@gmail.com

S. Ramya
Department of Information Technology
Skp engineering college
Thiruvannamalai, Tamilnadu, India.
E-mail-ramyasivaraman08@gmail.com

Abstract **-** Query Video has been send from base station to relay station. Base station sending video signal. And then user extract the video.Thus the video has been convert into several frame. Thus the video frame is covert into data conversion. Finally synchronization of the video frame.Hash code will be generation. This code can be used to the video secured purpose. Rijndael algorithm can be used to the formation of frame. Thus the encrypted conversion has been send from base station to relay station. Finally finding the RGB color.View conversion can be used to read the video data file. Calculate the time stamp, sequence,data length,and calculate the frame of the dimension(Width,Height). The proposed DTW-based synchronization method can achieve automatic synchronization for not only FH vectors, but also other types of video hashing methods. Shows the benefits of the proposed synchronization method to hash code generation. Again, the detection performance is significantly improved comparing with random recuperation.

Keywords **-** *hash code generation,Rijndael algorithm, DTW-based synchronization, finding the RGB color.*

*****

I. INTRODUCTION

There are many different computing and networking technologies — some available today, some just now emerging; some well-proven, some quite experimental. Understanding and solving today's computing dilemma more completely involves recognizing technologies; especially since a single technology by itself seldom suffices and, instead, multiple technologies are usually necessary. Some technologies are being obsoleted, some are maturing, some are adequate, and some are vital. A single and simple frame of reference is most helpful in understanding the concepts of individual networking technologies, seeing how they operate, and recognizing relationships among technologies. The various technologies share many fundamental concepts. This chapter provides an introduction to the world of networking technologies. It establishes a much generalized reference model, and then classifies technologies into categories relative to this model. A complete and generalized computing reference model is quite helpful in describing different technologies and their relationships. Many different groups in the computing industry have been involved during the last decade in developing computing reference models — some models for operating systems, some for data bases, some for application systems, and some for communications networking — but only recently have efforts begun in earnest to combine these various models into a single, more complete, but yet simpler reference model.

II. PROPOSED ALGORITHM

Data is encrypted using an encryption algorithm and an encryption key. This process generates ciphertext.Today's encryption algorithms are divided into two categories: symmetric and asymmetric. Symmetric-key encryption is much faster than asymmetric encryption, but the sender must exchange the key used to encrypt the data with the recipient before he or she can decrypt it. This requirement to securely distribute and manage large numbers of keys means most cryptographic processes use a symmetric algorithm to efficiently encrypt data, but use an asymmetric algorithm to exchange the secret key. Asymmetric cryptography, also known as public-key cryptography, uses two different but mathematically linked keys, one public and one private. The public key can be shared with everyone, whereas the private key must be kept secret. RSA is the most widely used asymmetric algorithm, partly because both the public and the private keys can encrypt a message; the opposite key from the one used to encrypt a message is used to decrypt it. This attribute provides a method of assuring not only confidentiality, but also the integrity, authenticity and non-reputability of electronic communications and data at rest through the use of digital signatures.

III. MODULES

A. Authority Identification

User send the input of original video Thus the video can be send from user to receiver. It can only identify the authorized user.It can specify some authority identification.Maintaining the Integrity of the Specifications

B. Hash code generation

A hash function is used to map data of arbitrary size to data of fixed size,returns by a hash function are called hash values, hash codes, hash sums, to map the search key to an index; the index gives the place in the hash table where the corresponding record should be stored.This requires that the hash function is collision resistant. These functions are categorized into cryptographic hash functions and provably secure hash functions. Functions in the second category are the most secure but also too slow for most practical purposes. Collision resistance is accomplished in part by generating very large hash values. For example SHA-1,

C. *Input query video*

User send the original video.Thus the video has been converted into some several fragmentation.

D. *View conversion*

Video has been splitted into some several frames. Each frame has been converted into some several data parts. Thus data has been send from user to receiver. The data requirements has been converted into all other frames.

E. *Rjindael process*

Video can be send from source to destination with secure by using rijndael algorithm.Data is encrypted using an encryption and key. This process generates ciphertext that can only be viewed in its original form if decrypted with the correct key. Decryption is simply the inverse of encryption.

F. *Color finding*

Finding the RGB color for each video frame. The color finding easily can formation of video's frame.he RGB color model is an additive color model.The main purpose of the RGB color model is for the sensing, representation, and display of images in electronic systems.Before the electronic age, the RGB color model already had a solid theory behind it, based in human perception of colors. RGB is a device-dependent color model.Thus an RGB value does not define the same color across devices without some kind of color management.

IV. SYSTEMARCHITECTURE

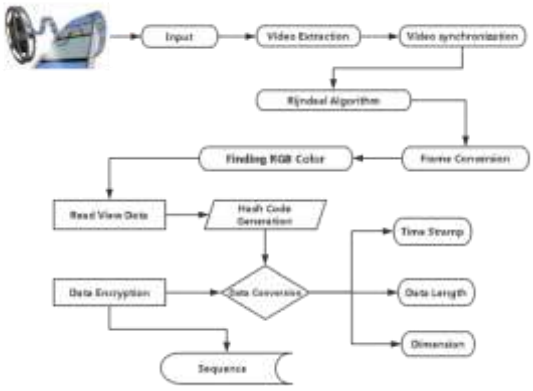

Figure 1:video frame conversion

CONCLUSION

video hashing framework that involves DTW based synchronization followed by computation of flow hash vectors. Further, distance boosting is proposed to capture complementary information in FH and DTW hash distances which delivers enhanced ROC performance even under severe spatio-temporal distortions. Future research can investigate computational aspects of synchronization and architectures/ techniques to speed up hash comparisons.A hash function is used to map digital data of arbitrary size to digital data of fixed size, returnes by a hash function are called hash values, hash codes, hash sums, or simply hashes. Query Video has been send from base station to relay station. Base station sending the video signal. And then user extract the video.Thus the video has been convert into several frame. Thus the video frame is covert into data conversion. Finally synchronization of the video frame.Hash code will be generation. This code can be used to the video secured purpose. Rijndael algorithm can be used to the formation of frame. Thus the encrypted conversion has been send from base station to relay station. Finally finding the RGB color.

REFERENCES

[1] C. De Roover, C. De Vleeschouwer, F. Lefebvre, and B. Macq, "Robust video hashing based on radial projections of key frames," IEEE Trans. Signal Processing, vol. 53, no. 10, pp. 4020 – 4037, Oct 2005.

[2] B. Coskun, B. Sankur, and N. Memon, "Spatio□temporal transform based video hashing," Multimedia, IEEE Transactions on, vol. 8, no. 6,pp. 1190 –1208, 2006.

[3] Sunil Lee and C.D. Yoo, "Robust video fingerprinting for content-based video identification," Circuits and Systems for Video Technology, IEEE Transactions on, vol. 18, no. 7, pp. 983 –988, july 2008.

[4] M.M. Esmaeili, M. Fatourechi, and R.K. Ward, "A robust and fast video copy detection system using content-based fingerprinting," Information Forensics and Security, IEEE Transactions on, vol. 6, no. 1, pp. 213–226, 2011.

[5] R. Chaudhry, A. Ravichandran, G. Hager, and R. Vidal, "Histograms oriented optical flow and binet-cauchy kernels on nonlinear dynamical systems for the recognition of human actions," in Computer Vision and Pattern Recognition, 2009. CVPR 2009. IEEE Conference on, 2009, pp.1932–1939.

[6] Y.J. Ren, L. O'Gorman, L.J. Wu, Fangzhe Chang, T.L. Wood, and J.R.Zhang, "Authenticating lossy surveillance video," Information Forensics and Security, IEEE Transactions on, vol. 8, no. 10, pp. 1678–1687, 2013.

[7] Jennifer Ren, Fangzhe Chang, Thomas Wood, and John R. Zhang,"Efficient video copy detection via aligning video signature time series,"in Proceedings of the 2Nd ACM International Conference on Multimedia Retrieval, New York, NY, USA, 2012, ICMR '12, pp. 14:1–14:8, ACM.

[8] J.R. Zhang, J.Y. Ren, Fangzhe Chang, T.L. Wood, and J.R. Kender,"Fast near-duplicate video retrieval via motion time series matching," in Multimedia and Expo (ICME), 2012 IEEE International Conference on, 2012, pp. 842–847.

[9] Zi Huang, Heng Tao Shen, Jie Shao, Bin Cui, and Xiaofang Zhou,"Practical online near-duplicate subsequence detection for continuous video streams," Multimedia, IEEE Transactions on, vol. 12, no. 5, pp.386–398, 2010.

[10] Jiajun Liu, Zi Huang, Heng Tao Shen, and Bin Cui, "Correlation-based retrieval for heavily changed near-duplicate videos," ACM Transactions on Information Systems (TOIS), vol. 29, no. 4, pp. 21, 2011.