Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 2, February 2014, pg.483 – 489

RESEARCH ARTICLE

JOINT VIDEO COMPRESSION AND ENCRYPTION USING SECURE WAVELET TRANSFORM AND ENTROPY CODING

[1]E.Mallika, [2]K.SivaKumar

[1]PG scholar, Department of Computer Science and Engineering, Anna University Chennai, India
[2]Assistant Professor, Department of Computer Science and Engineering, Anna University Chennai, India
[1,2]Roever Engineering College, Perambalur
[1] mallikamecse@gmail.com, [2] hod_cse@roeverengg.edu.in

Abstract- Algorithmic parameterization and hardware architectures can ensure secure transmission of multimedia data in resource constrained environments such as wireless video surveillance networks, telemedicine frameworks for distant health care support in rural areas, and Internet video streaming. Joint multimedia compression and encryption techniques can significantly reduce the computational requirements of video processing systems. To reduce the computational cost of multimedia encryption, along preserving the properties of compressed video (useful for scalability, and transcoding, and retrieval), which endanger loss by naive encryption. In this system, express the two compression blocks for video coding - a modified frequency transform called as Secure Wavelet Transform or SWT and a modified entropy coding scheme called Chaotic Arithmetic Coding (CAC) is used for video encryption. Experimental results are shown for selective encryption using proposed schemes. The SWT has rational coefficients which allow us to build a high throughput hardware implementation on fixed point arithmetic. In CAC, a large number of chaotic maps can be used to perform coding, each achieving Shannon optimal compression performance.

Keywords: Compression, Frame Extraction, Secure Wavelet Transform, Encryption, Entropy coding.

I. INTRODUCTION

The design of algorithms and the hardware architectures for secure transmission of multimedia data in resource-constrained environments. Conventional encryption schemes such as those using DES is suitable for video data because of the large computational overhead. Compressed multimedia streams also exhibit well defined hierarchical structure that can be exploited in several useful ways e.g. scalability, random access, trans-coding, rate shaping in low and variable bandwidth scenarios these structures would be recognizable in traditional cipher text.

An augmented video coding model is used for joint compression and encryption which can significantly reduce the computational requirements. To build design blocks which enable security for these applications at the algorithmic level, and leave domain-specific optimization to application developers. These algorithmic optimizations map easily to fixed point hardware, allowing us to come up with efficient architectural optimizations for resource constrained scenarios. In other application scenarios, these approaches can complement the security provided by conventional schemes such as AES.

The proposed schemes are also low-cost in the sense that the required computational cost is considerably smaller than existing approaches, and in some configurations resources are fewer than that for conventional video compression schemes.

1.1 Compression

Compression is driven by the cost of wide area network access and user demands for increased bandwidth. The cost of WAN access is a significant part of the cost of providing a data network and the use of data compression on networks can result in significant savings. Compression increases the effective throughput of data across a network link by reducing the size of packets. This lets more packets be transmitted over links in the same time interval, or the same number of packets can be transmitted over a slower and cheaper link in the same time interval.

Compression identifies redundancy in the data and produces an encoded form that is smaller, yet contains all the information required to recreate the original data. This is called lossless data compression, as opposed to voice and video compression which, due to their analog nature, normally use lossy data compression algorithms. Most modern high performance data compression techniques use variations of the Lempel-Ziv algorithm. This algorithm compresses data by maintaining data histories at the compression and decompression ends of the link. These histories contain the most recent data transmitted on a data link.

1.2 Encryption

Encryption for routers is driven by the need for organizations to keep sensitive data private and secure. Encrypting network data before it is passed to the wide area network ensures that the data cannot be read or modified as it traverses the WAN. Since all wide area traffic passes through the

router, the router is the ideal place to locate the complex hardware required to provide secure data encryption. Locating the encryption function in the network router and integrating the complex encryption key management procedures into the router's management system minimizes the cost of supporting an encrypted network.

Data encryption operates by applying an encryption algorithm and key to the original data the plaintext to convert it into an encrypted form the ciphertext. The ciphertext produced by encryption is a function of the algorithm used and the key. Since it is easy to discover what type of algorithm is being used the security of an encryption system relies on the secrecy of its key information. When the ciphertext is received by the remote router the decryption algorithm and key are used to recover the original plaintext.

II. PROPOSED WORK

Securing a multimedia content using joint compression and encryption. An augmented video coding model is used for joint compression and encryption which can significantly reduce the computational requirements. A modified frequency transform (called as Secure Wavelet Transform or SWT) and a modified entropy coding scheme, (called Chaotic Arithmetic Coding (CAC)) can be used for video encryption. Arithmetic coding is especially suitable for small alphabet binary sources with highly skewed probabilities. Arithmetic coding is very popular in the image and video compression applications.

Peak Signal to Noise Ratio (PSNR)

The phrase peak signal-to-noise ratio, often abbreviated PSNR, is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. Because many signals have a very wide dynamic range, PSNR is usually expressed in terms of the logarithmic decibel scale. The PSNR is most commonly used as a measure of quality of reconstruction of lossy compression codec's (e.g., for image compression). The signal in this case is the original data, and the noise is the error introduced by compression.

The PSNR value is defined as:

PSNR = 10.log(-----)

PSNR = 20.log(------)

Calculate Average PSNR/MSE Value

The Average Value of PSNR for SWT as shown in Table-1.

Table-1:

Average value of PSNR for SWT

VALUE	SWT
AVERAGE PSNR	0.0056

III. SYSTEM DESIGN

The architecture of the proposed system is shown in fig.2.1.The system jointly addresses the compression and encryption techniques, which are explained below.

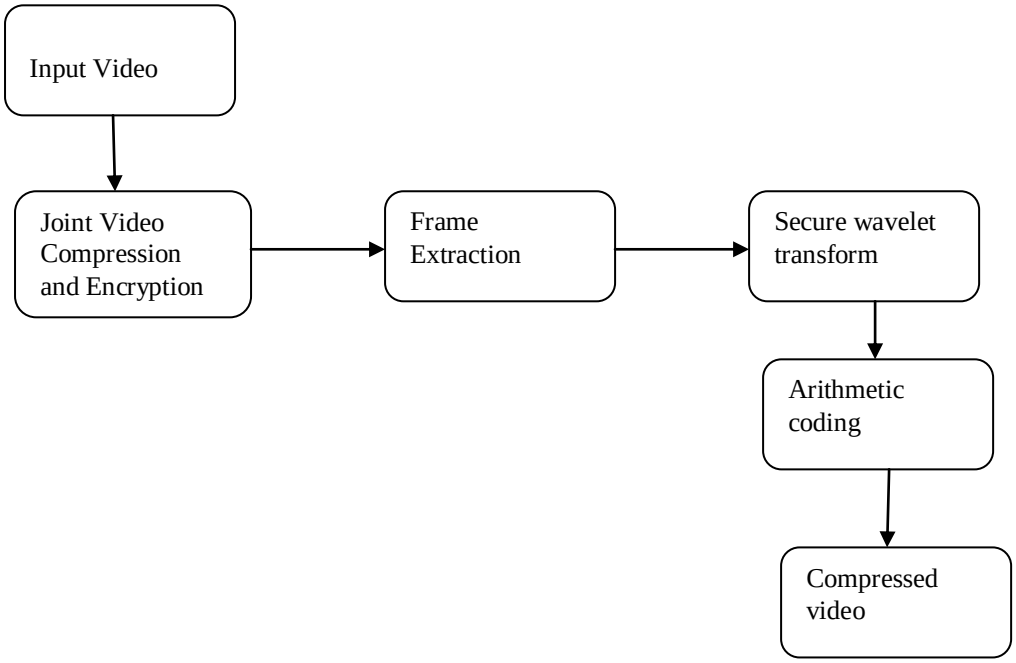


Fig.3.1 System Architecture

First the videos are initialized and converted into avi format. The converted videos are extracted into frames. The sender choose the lossy algorithm i.e., an augmented video coding model, which is used for joint compression. Compression is the process of coding that will effectively reduce the total number of bits needed to represent certain information. It contains the spatial model, prediction model and entropy encoding. The spatial model parameterize the transform filters such that the choice of filter depends on key value.

The prediction model use a fuzzy prediction model, which selects from several past and future frames and uses multiple stream based on a key-dependent fuzzy logic instead of the traditional use of immediate neighbors. Entropy coding can be used with multiple statistical models so that exact choice

of model is governed by a key. Special application of general encryption to multimedia such that the content cannot be rendered intelligibly or to an acceptable perceptual quality. Among the number of frames are required an order of priorities. In receiver side received, the video in unknown format. It leads to provide security in transmission. Receiver decrypt the received video using asymmetrical key. Decomposition of decrypted video is done in either decompression algorithm to retrieve original transmitted video from sender. Evaluate the performance based on SWT and CAC.

Table 2

Improved image reconstruction (PSNR values) with hardware-amenable SWT implementation

Image		Bit rate			Bitrate	
	Daub. 9/7	SWT	Martina	Daub.9/7	SWT	Martina
lena	28.213	29.46	27.7	38.47	38.17	36.5
survillance	2.61	28.1	26.54	38.41	42.21	37.21
lecture	34.35	33.8	32.73	48.3	51.25	43.71
helicoptor	33.75	35.72	35.01	48.5	54.72	47.14

IV. FRAME EXTRACTION

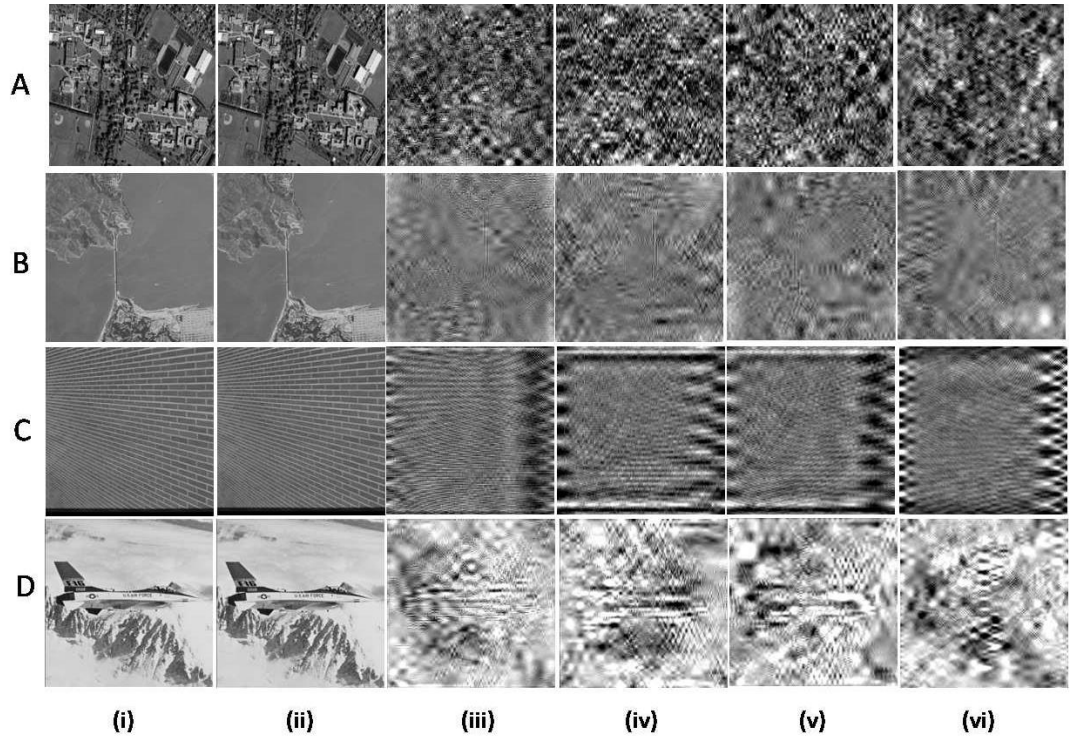
Frame extraction module is responsible for read the input video and extracts the number of frames from that video. The background of the image, want to extract is roughly all one color, use the Fuzzy select tool and put the threshold at just high enough to select everything.

V. SECURE WAVELET TRANSFORM

Secure Wavelet Transform is responsible for the video encryption scheme secure wavelet transform is applied. It is a light weight multimedia encryption strategy based on a modified Discrete Wavelet Transform (DWT). The SWT provides joint multimedia encryption and compression by two modifications: parameterized construction of the DWT and re-orientation for the wavelet decomposition. The SWT has rational coefficients which allow us to build a high throughput hardware implementation on fixed point arithmetic.

VI. CHAOTIC ARITHMETIC CODING

Arithmetic coding is responsible for data encryption scheme based on arithmetic coding called chaotic arithmetic coding is applied. CAC uses a key to make the exact choice of map from the family of predefined maps to perform AC. Arithmetic Coding (AC) is widely used for the entropy coding of text and multimedia data. It involves recursive partitioning of the range (0,1) in accordance with the relative probabilities of occurrence of the input symbols. In CAC, a large number of chaotic maps can be used to perform coding, each achieving Shannon-optimal compression performance.



VII. SIMULATION WORK

The simulation results of video compression by applying the secure wavelet transform(SWT) algorithm. The original video can be split in the form of frames and compressed it. After applying the SWT algorithm on original frame it reduces the PSNR and MSE values.

VIII. CONCLUSION

The system architecture is based on joint compression and encryption schemes for securing the multimedia content. To provide the potential for hardware savings and efficient encryption using this design with two examples - Secure Wavelet Transform and Chaotic Arithmetic Coding. To improve the deployment in state-of-the-art video codes such as H.264/ SVC. There is possibility of developing such encryption schemes for motion compensation and estimation, and implementation on embedded device architecture.

REFERENCES

[1]. G. Gualdi, A. Prati, and R. Cucchiara, "*Video streaming for mobile video surveillance*," *Multimedia, IEEE Transactions* on, vol. 10, no. 6, pp. 1142 –1154, Oct. 2008.

[2]. .R. Bose and S. Pathak, "*A novel compression and encryption scheme using variable model arithmetic coding and coupled chaotic system," IEEE Trans. Circuits and Systems* I, vol. 53, no. 4, pp. 848–857, April 2006.

[3]. A. Pande and J. Zambreno, "*Poly-DWT: Polymorphic wavelet hardware support for dynamic image compression," ACM Transactions on Embedded Computing Systems*, vol. 10, no. 6, pp. 1142 –1154, Oct. 2011.

[4]. G.Jakimoski and K. Subbalakshmi, "*Cryptanalysis of some multimedia encryption schemes," IEEE Trans. Multimedia*, vol. 10, no. 3, pp. 330–338, April 2008.

[5]. H. Kim, J. Wen, and J. Villasenor, "*Secure arithmetic coding,"IEEE Trans. Signal Processing*, vol.55, no. 5, pp.May 2007.

[6]. O. Oyman, J. Foerster, Y. joo Tcha, and S.-C. Lee, "*Toward enhanced mobile video services over wimax and lte [wimax/lte update]," Communications Magazine, IEEE,* vol. 48, no. 8, pp. 68 –76, Aug. 2010.

[7]. M. Baugher, D. McGrew, M. Naslund, E. Carrara, and K. Norrman, "*The secure real-time transport protocol (SRTP),*" UnitedStates, 2004.

[8]. C. E. Shannon, "*Communication theory of secrecy systems,"Bell Systems Technical Journal*, vol. 28, pp. 656– 715, 1949.

[9] D. I. Cohen A. and F. J.C., "*Biorthogonal Bases of Compactly Supported Wavelets*," *Commun. Pure Appl. Math.*, vol. 45, pp.485–560, 1992.

[10] A. Pande and J. Zambreno, "*Poly-DWT: Polymorphic wavelet hardware support for dynamic image compression*," *ACM Transactions on Embedded Computing Systems*, 2011.

[11] D. Engel and A. Uhl, "*Parameterized biorthogonal wavelet lifting for lightweight JPEG 2000 transparent encryption,"* in *Proc. ACM Work. on Multimedia and Security (MM&Sec) 2005*. ACM, 2005, pp. 63–70.

[12]. Z. Liu and N. Zheng, "*Parametrization construction of biorthogonal wavelet filter banks for image coding," Springer Signal, Image and Video Processing*, vol. 1, no. 1, pp. 63–76, 2007.

[13]. N. Nagaraj and P. G. Vaidya, "*One-time pad, arithmetic coding and logic gates: An unifying theme using dynamical systems," CoRR*, vol. abs/0803.0046, 2008.

[14] . A. Pande, P. Mohapatra, and J. Zambreno, "*Using chaotic maps for encrypting image and video content," in IEEE International Symposium of Multimedia*, 2011, pp. 171 – 178

Authors Profile

E. Mallika – Currently pursuing her M.E in Computer Science and Engineering from Roever Engineering College, Perambalur. Her areas of interest are network security, and Mobile computing.

K. SivaKumar – He is working as an Assistant Professor in Dept.of Computer Science and Engineering in Roever Engineering College, Perambalur, India. His areas of interest are network security, Mobile computing, and Cloud computing.

