Comparative Study of Partial Encryption of Images and Video

Ms. A.Anto Steffi*, Mr. Dipesh Sharma**

*(Department of Computer Science & Engg., RIT Raipur, Chhattisgarh, India)

** (Department of Computer Science & Engg., RIT Raipur, Chhattisgarh, India)

ABSTRACT

The traffic of digital images and video has grown rapidly in the internet. Security becomes important for several applications like military image database, confidential video conferencing, medical images, etc. Several techniques have been developed for textual data but are not appropriate for images and video with huge amount of file size. Partial encryption is a recent approach to reduce the encryption time of images and video in distributed network. Partial encryption scheme encrypts a portion of compressed bit stream. In this paper we compare and classified various proposed partial encryption schemes for images and video.

Keywords **-** Compression, JPEG, MPEG, Partial Encryption

1. INTRODUCTION

The increased popularity of multimedia applications has demanded a certain level of security. In some applications, it is relevant to hide the content of a message when it enters an insecure channel. The initial message prepared by the sender is then converted into cipher text prior to transmission. The process of converting plain text into cipher text is called encryption. The encryption process requires an encryption algorithm and a key. The process of recovering plain text from cipher text is called decryption. Because common encryption methods generally manipulate an entire data set, most encryption algorithms tend to make transfer of information more costly in terms of time and sometimes bandwidth. Traditionally, an appropriate compression algorithm is applied to the multimedia data and its output is encrypted by an independent encryption algorithm. This process must be reversed by the receiver.

Unfortunately, the processing time for encryption and decryption is a major factor in real-time image communication. In addition, the processing time required for compression and decompression of an associated image data is important. Encryption and decryption algorithms are too slow to handle the tremendous amount of data transmitted. One difference between text data and image data is that the size of image data is much larger than the text data. The time is a very important factor for the image encryption. We find it at two levels, one is the time to encrypt, the other is the time to transfer images. To minimize the time, the first step is to choose a robust, rapid and easy method to implement cryptosystem. The other important criteria concerns the method of compression is that to decrease the size of images without loss of image quality [1]. One possible solution is a system of partial encryption, encrypting only the smallest portion of the data that makes the entire data set unusable. Partial encryption is a recent approach to reduce the computational requirements for huge volumes of multimedia data. Partial encryption is currently an important research area. We will start with a classification and brief description of the proposed schemes in order to identify some of the related problems.

2. PARTIAL ENCRYPTION

The encryption algorithms, which have been originally developed for text data, are not suitable for securing many real time algorithms, which have been originally developed for text data, are not suitable for securing many real time multimedia applications because of large data sizes. Software implementations of ciphers are usually too slow to process image and video data in commercial systems. Hardware implementations, on the other hand, add more cost to service providers and consumer electronics device manufacturers. Recent trend is to minimize the computational requirements for secure multimedia distribution by “partial encryption” where only parts of the data are encrypted.

2.1 Partial Encryption Schemes for Images

- Cheng and Li, 2000

  Cheng and Li [2] proposed partial encryption methods that are suitable for images compressed with two specific classes of compression algorithms:

  a) quad tree image compression algorithms

  It allows the encryption and decryption time to be significantly reduced without affecting the compression performance of the underlying compression algorithm. In this scheme, the compression output is partitioned into two parts; one is important and other is unimportant parts. Important parts provide a significant amount of information about original data, whereas remaining part called unimportant parts may not provide much information without important parts. Encryption will only perform for important parts. A significant reduction in encryption and decryption time is achieved when the relative size of important part is small. This scheme is not tunable as static parameters are encrypted. High visual degradation can be achieved only with image having high information rate. As encryption is performed after compression, so no impact is observed on compression efficiency. Encryption ratio can vary from 14% to 50%. Brute force attack is possible for low information images where quad tree structure is very simple. So the security level of this scheme is low.

  b) Wavelet compression based on zero trees

  In general, wavelet compression algorithms based on zero trees transmit the structure of the zero tree with the significant coefficients. The SPIHT algorithm, for example, transmits the significance of the coefficient sets that correspond to trees of coefficients. Among the many different types of bits generated by the SPIHT algorithm, the proposed partial encryption scheme encrypts only the significance information related to pixels or sets in the two highest pyramid levels in addition to the parameter *n* that determines the initial threshold.

- Droogenbroeck and Benedett, 2002

  a) Proposed selective encryption methods for raster images and JPEG images. In their method the DC coefficients are not ciphered because they carry important visible information and they are highly predictable. Moreover, in their approach the compression and encryption stages are separated and that requires an additional operating cost [3].

  b) This method is proposed for uncompressed image, which applies to a binary image, consist in mixing image data and a message (key) that has the same size as the image: a XOR function is sufficient when the message is only used once. A generalization to gray level images is straightforward: Encrypt each bit plane separately and reconstruct gray level image. With this approach no distinction between bit planes is introduced although the subjective relevance of each bit plane is not equal. The highest bit planes exhibit some similarities with the gray level image, but the least significant bit planes look random. Because encrypted bits also look random, the encryption of least significant bit planes will add noise to the image. The advantage of least significant bits is that plaintext attacks are harder on random like data. It is preferable to encrypt bits that look most random. This scheme is tunable. Very high visual degradation can be achieved by encrypting 4 to 5 bit planes. This technique is used for uncompress image so no impact is observed on compression efficiency. In this scheme encryption ratio vary from 50 to 60%. It is fast as XOR operation takes less time. It is not robust against cryptanalysis attack. So, security level is low.

- Podesser, Schmitdt and Uhl, 2002

  In selective bit plane encryption using AES is proposed. Several experiments were conducted on 8 bit grayscale images, and the main results retained are following: 1. encrypting only the

MSB is not secure; a replacement attack is possible 2. Encrypting the first two MSBs gives hard visual degradation, and 3. Encrypting three bit planes gives very hard visual degradation. This scheme is not tunable as fix number of bits are encrypted. For 8 bits per pixel uncompressed image, hard visual degradation (of 9 d B) can be observed for a minimum of 3MSB bits encrypted. This scheme is intended for uncompressed data. Encryption can increase data size so it is not compression friendly. In this scheme encryption is performed before compression, so it is format compliant. At least 3 bit planes over 8 (more than 37.5%) of the bit stream have to be encrypted using AES to achieve sufficient security even when a secure cipher is used (AES), the selective encryption algorithm proposed is vulnerable to replacement attacks. This attack does not break AES but replaces the encrypted data with an intelligible one. It is worth to note that visual distortion is a subjective criterion and does not allow to measure security as illustrated in this example. Security level of this technique can be scaled as medium [4].

- Pommer and Uhl, 2003

The authors proposed wavelet packet based compression instead of pyramidal compression schemes in order to provide confidentiality. Header information of a wavelet packet image coding scheme that is based on either a uniform scalar quantizer or zero trees is protected: it uses AES to encrypt only the sub band decomposition structure. In this approach the encoder uses different decomposition schemes with respect to the wavelet packet sub band structure for each image. it is based on AES encryption of the header information of wavelet packet encoding of an image, this header specifies the sub band tree structure. These decomposition trees are encrypted and have to be present at the decoder to be able to reconstruct the image data properly. The advantage in comparison to other selective encryption approaches is that the amount of necessary encryption is extremely small since only header information, and no visual data, needs to be processed. It is not tunable. The encrypted content cannot be viewed without decryption. The sub band tree is pseudo randomly generated. This adversely impacts the compression efficiency. It is not format compliant. The encrypted part represents a very small fraction of the bit stream. It is not secure against chosen plaintext attack. Because statistical properties of wavelet coefficients are preserved by the encryption, then the approximation sub band can be reconstructed. This will give the attacker the size of the approximation sub band (lower resolution) and then neighbouring sub bands can be reconstructed since close sub bands contain highly correlated coefficients [5].

2.2 Partial Encryption Schemes for Video

- Meyer and Gadegast, 1995

This methodology is proposed for MPEG videos. This method uses traditional encryption methods RSA or DES in CBC mode to encrypt MPEG video stream. It implements 4 level of security. (i) Encrypting all stream headers. (ii) Encrypting all stream headers and all DC and lower AC coefficients of intracoded blocks. (iii) Encrypting I-frames and all I-blocks in P- and B frames.(iv) Encrypting all the bit streams. The number of I blocks in P or B frames can be of the same order as the number of I blocks in I frames. This reduces considerably the efficiency of the selective encryption scheme. Encryption ratio may vary based on which parameters are encrypted. Encrypting only headers have very less encryption ratio. But encrypting all the bit streams have 100% encryption ratio. Speed of this methodology again varies based on traditional algorithm in use such as DES or RSA and number of parameters that are encrypted. Many security levels can be obtained. Encrypting only stream headers is not sufficient since this part is easily predictable. But encrypting all the bit streams can provide high security. Detailed cryptanalysis of this methodology is not defined. A special encoder and decoder are required to read unencrypted SECMPEG stream. The encoder proposed is not MPEG compliant [6].

- Spanos and Maples, 1995

Aegis mechanism is proposed. It encrypts intraframes, video stream header and the ISO 32 bits end code of the MPEG stream using DES in CBC mode. Experimental results were conducted by the authors showing the importance of selective encryption in high bit rate video transmission to achieve acceptable end-to-end delay. It is also shown that full encryption creates bottleneck in high bit rate distributed video applications. Agi and Gong showed that this algorithm has low security since encrypting of only I-frames offer limited security because of the intercorrelation of frames; some blocks are intracoded in P and B frames. Furthermore, P and B-frames are highly correlated when they correspond to the same I-frame. They also underlined that it is unwise to encrypt stream headers since they are predictable and can be broken by plaintext-cipher text pairs. Alatter and Al-ragib, apparently unaware of Agi and Gong work, stressed the same security leakage. Encryption is performed after compression, thus no impact is observed on the compression efficiency. The resulting bit stream is not MPEG compliant [7].

- Shi and Bhargava, 1998

The authors [8] proposed video encryption algorithm (VEA) which uses a secret key to randomly change the signs of all DCT coefficients in an MPEG stream. It is fast as it operates on a small portion of original video. It is more efficient than DES algorithm because it only selectively encrypts a small number of bits of the MPEG compressed video and selected bit is only XORed one time with the corresponding bit of the secret key. VEA does not protect from plaintext attack provided the attacker knows the original video image (plaintext and cipher text). The authors present a new version of VEA reducing computational complexity; it encrypts the sign bits of differential values of DC coefficients of I-frames and sign bits of differential values of motion vectors of Band P-frames. This type of improvement makes the video playback more random and more non viewable. When the sign bits of differential values of motion vectors are changed, the directions of motion vectors change as well. In addition, the magnitude of motion vectors change, making the whole video very chaotic. Modified VEA encrypt DC coefficients of I frame, and leave AC coefficients of I frames unchanged. Thus it significantly reduces encryption computations. Because DC coefficients of I frames are differentially encoded, changing a few sign bits of differential values of DC coefficients will affect many DC coefficients during MPEG decoding. MPEG's differential code of DC coefficients and motion vectors increase the difficulty to break MVEA encrypted videos. The first version of VEA [21] is only secure if the secret key is used once. Otherwise, knowing one plaintext and the corresponding cipher text, the secret key can be computed by XORing the DCT sign bits. Both versions of VEA are vulnerable to chosen plaintext attacks; it is feasible to create a repetitive/periodic pattern and then compute its inverse DCT. The encryption of the image obtained will allow us to get the key length and even compute the secret key by chosen-plaintext attack.

- Shi, Wang and Bhargava, 1999

A new version of the modified VEA presented is proposed, called real time video encryption algorithm (RVEA) [9]. It encrypts selected sign bits of the DC coefficients and/or sign bits of motion vectors using DES or IDEA. It selects at most 64 sign bits from each macro block. RVEA achieves the goal of reducing and bounding its computation time by limiting the maximum number of bits selected. The differential encoding of DC coefficients and motion vectors in MPEG compression increases difficulty of breaking RVEA encrypted videos. If the initial guess of a DC coefficient wrong, it is very difficult to guess the following DC values correctly.

- Wu and Kuo, 2001

It [10] is based on a set of observations, the authors point out that energy concentration does not mean intelligibility concentration. Indeed, they discussed the technique proposed by Tang. They show that by fixing DC values at a fixed value and recovering AC coefficients (by known or chosen plaintext attacks), a semantically good reconstruction of the image is obtained. Even using a very small fraction of the AC coefficients does not fully destroy the image semantic content. The authors argued that both orthogonal transform-based compression algorithms followed by quantization and compression algorithms that end with an entropy coder stage are bad candidates to selective encryption. They investigate another approach that turns entropy coders into ciphers. They propose two schemes for the most popular entropy coders: multiple Huffman tables (MHTs) for the Huffman coder and multiple state index (MSI) for the QM arithmetic coder.

MHT*:* The authors propose a method using multiple Huffman coding tables. The input data stream is encoded using multiple Huffman tables. The content of these tables and the order that they are used are kept secret as the key for decryption. In the proposed system, instead of training thousands of Huffman coding tables, it only train and obtained four different Huffman tables. Then, thousands of different tables can be derived using a technique called Huffman tree mutation. Gillman and Rivest showed that decoding a Huffman coded bit stream without any knowledge about the Huffman coding tables would be very difficult. However, the basic MHT is vulnerable to known and chosen plaintext attacks.

MSI*:* The arithmetic QM coder is based on an initial state index; the idea is to select 4 published initial state indices and to use them in a random but secret order. Unlike Huffman coding with a fixed and pre defined Huffman tree, the QM coder dynamically adjusts the underlying statistical model to a sequence of received binary symbols. It is very difficult to decode the bit stream without the knowledge of the state index used to initialize the MQcoder. A little effect on compression efficiency is observed. This is due to multiple initializations of the QM coder due to initial state index changing.

- Wen, Severa, Zeng,Luttrel, and Jin, 2002

A general selective encryption approach for fixed and variable length codes (FLC and VLC) is proposed in [11].FLC and VLC codewords corresponding to important information carrying fields are selected. Then, each codeword in the VLC and FLC (if the FLC code space is not full) table is assigned a fixed length code index, when we want to encrypt the concatenation of some VLC (or FLC) codewords, only the indices are encrypted (using DES). Then the encrypted concatenated indices are mapped back to a different but existing VLC. The encryption process compromises the compression efficiency. Indeed, some short VLC codewords (which are the most probable/frequent) can be replaced by longer ones. This is antagonistic with the entropy coding idea. The proposed scheme is fully compliant to any compression algorithm that uses VLC or FLC entropy coder.

- Zeng and Lei, 2003

In [12], selective encryption in the frequency domain (8×8 DCT and wavelet domains) is proposed. The general scheme consists of selective scrambling of coefficients by using different primitives such as selective bit scrambling, block shuffling, and/or rotation. In wavelet transform case selective bit scrambling and block shuffling is done. In selective bit scrambling the first nonzero magnitude bit and all subsequent zero bits if any give a range for the coefficient value. These bits have low entropy and thus highly compressible and all remaining bits called refinement bits are uncorrelated with the neighbouring coefficients. In this scheme, sign bits and refinement bits are scrambled. In block shuffling, the basic idea is to shuffle the arrangement of coefficients within a block in a way to preserve some spatial correlation; this can achieve sufficient security without compromising compression efficiency. Each subband is split into equal-sized blocks. Within the same subband, block coefficients are shuffled according to a shuffling table generated using a secret key. Since the shuffling is block based, it is expected that most 2D local subband statistics are preserved and compression not greatly impacted.

In DCT transform case, the 8 × 8 DCT coefficients can be considered as individual local frequency components located at some subband. The block shuffling and sign bits change can be applied on these “subbands.” I, B, and P frames are processed in different manners. For I-frames, the image is first split into segments of macroblocks, blocks/macroblocks of a segment can be spatially disjoint and chosen at random spatial positions within the frame. Within each segment, DCT coefficients at the same frequency location are shuffled together. Then, sign bits of AC coefficients and DC coefficients are randomly changed. There may be many intracoded blocks in P- and B-frames. At least DCT coefficients of the same intracoded block in P- or B-frames are shuffled. Sign bits of motion vectors are also scrambled. It is vulnerable to chosen and known plaintext attacks since it is based only on permutations. In addition, replacing the DC coefficients with a fixed value still gives an intelligible version of the image. This algorithm can be part of permutation based encryption.

- Bergeron and Lamy-Bergot, 2005

A syntax compliant encryption algorithm is proposed for H.264/AVC [13]. Encryption is inserted within the encoder. Using the proposed method allows to insert the encryption mechanism inside the video encoder, providing a secure transmission which does not alter the transmission process. The bits "selected for encryption" are chosen with respect to the considered video standard according to the following rule: each of their encrypted configurations gives a non-desynchronized and fully standard compliant bit stream. This can in particular be done by encrypting only parts of the bit stream which have no or a negligible impact in evolution of the decoding process, and whose impact is consequently purely a visual one. About 25% of I-slices and 10–15% of P-slices are encrypted. Since intracoded slices can represent 30–60%, the encryption ratio is expected to be relatively high. The main drawback of this scheme is the lack of cryptographic security. Indeed, the security of the encrypted bit stream does not depend more on the AES cipher. It depends on the size of the compliant codewords. Hence, the diffusion of the AES cipher is reduced to the plaintext space size. In addition, a bias is introduced in the cipher text. This bias depends on the key size and the plaintext space size.

- Lian, Liu, Ren and Wang, 2006

This scheme is proposed for AVC [14]. During AVC encoding, such sensitive data as intra prediction mode, residue data and motion vector are encrypted partially.
Among them, intra prediction mode is encrypted based on exp-golomb entropy coding, the intra macroblocks DCs are encrypted based on context based adaptive
variable length coding, and intra macroblocks ACs and the inter macroblocks MVDs are sign encrypted with a stream cipher followed with variable length coding. The encryption scheme is of high key sensitivity, which means that slight difference in the key causes great differences in cipher video and that makes statistical or differential attack difficult. It is difficult to apply known plaintext attack. In this encryption scheme, each slice is encrypted under the control of a 128 bit sub-key. Thus, for each slice, the brute force space is 2^128; for the whole video, the brute force space is 2^256 (the user key is of 256 bit). This brute force space is too large for attackers to break the cryptosystem. According to the encryption scheme proposed here, both the texture information and the motion information are encrypted, which make it difficult to recognize the texture and motion information in the video frames.

3. CONCLUSION

Although an important and rich variety of encryption algorithms have been proposed in literature, most of the algorithms are not secure against cryptanalytic attack. So these algorithms are not suitable for applications which demand high security. It is difficult for a single algorithm to satisfy all performance parameters. We can conclude that it is a challenge for researchers to design an encryption algorithm which satisfies all parameters like visual degradation, speed, encryption ratio, compression friendliness and cryptographic security. Promising future directions of research include more emphasis on key management, resolving the conflict between compression and encryption, and finding ways to change the selection criteria dynamically. Moreover, none of the techniques have used Elliptic curve cryptography, hybrid encryption algorithm

ACKNOWLEDGEMENTS

We give special thanks to Mrs.Uzma, HOD, Department of Computer Science & Engg., RIT Raipur, Chhattisgarh, India, Whose feedback helped me to improve my article.

References

[1] Borie J., Puech W., and Dumas M.,"Crypto-Compression System for Secure Transfer of Medical Images", *2nd International Conference on Advances in Medical Signal and Information Processing (MEDSIP 2004),* September 2004

[2] H. Cheng and X. Li, "*Partial Encryption of Compressed Images and Video*," IEEE Transactions on Signal Processing, 48(8), 2000, pp. 2439-2451.

[3] M. Van Droogenbroeck and R. Benedett, "*Techniques for a Selective Encryption of*

Uncompressed and Compressed Images," Proceedings of Advanced Concepts for Intelligent Vision Systems (ACIVS) 2002, Ghent, Belgium, September 9-11, 2002.

[4] M. Podesser, H.-P. Schmidt and A. Uhl, "Selective Bitplane Encryption for Secure Transmission of Image Data in Mobile Environments," *5th Nordic Signal Processing Symposium, on board Hurtigruten, Norway, October 4-7*, 2002.

[5] A. Pommer and A. Uhl, "Selective Encryption of Waveletpacket Encoded Image Data: Efficiency and Security,"Multimedia Systems, Vol. 9, No. 3, 2003, pp. 279–287, DOI: 10.1007/s00530-003-0099-y.

[6] J. Meyer and F. Gadegast, "Security Mechanisms for Multimedia Data with the Example MPEG-1 video," Project Description of SECMPEG, Technical University of Berlin, 1995.

[7] G.A. Spanos and T.B.Maples, "Performance Study of a Selective Encryption Scheme for the Security of Networked Real Time Video," in *Proceedings of the International Conference on Computer Communications and Networks,1995, pp. 2-10.*

[8] C. Shi and B. Bhargava, "A Fast MPEG Video Encryption Algorithm," *in Proceedings of the 6th ACM International Conference on Multimedia, 1998, pp. 81–88.*

[9] C. Shi, S. Y.Wang, and B. Bhargava, "MPEG Video Encryption in Real-time using Secret Key Cryptography," in *Proceedings of the International Conference on Parallel and Distributed Processing Algorithms and Applications, 1999,pp. 191–201.*

[10] C.-P. Wu and C.-C. J. Kuo, "Fast Encryption Methods for Audiovisual Data Confidentiality," in *Proceedings of SPIE, 2001, Vol. 4209, pp. 284–295.*

[11] J. Wen, M. Severa, W. Zeng, M. H. Luttrell, and W. Jin, "A Format-Compliant Configurable Encryption Framework for Access Control of Video," IEEE Transactions on Circuits and Systems for Video Technology, Vol. 12, No. 6, 2002, pp. 545–557.

[12] W. Zeng and S. Lei, "Efficient Frequency Domain Selective Scrambling of Digital Video," IEEE Transactions on Multimedia, Vol. 5, No. 1, 2003, pp. 118–129.

[13] C. Bergeron and C. Lamy-Bergot, "Compliant Selective Encryption for H.264/AVC Video Streams," in Proceedings of the 7th IEEE Workshop on Multimedia Signal Processing ,2005, pp. 1–4.

[14] Shiguo Lian, Zhongxuan Liu, Zhen Ren and Haila Wang, "Secure Advanced Video Coding Based on Selective Encryption Algorithms," IEEE Transaction on Consumer Electronics, Vol. 52, No. 2 ,2006, pp. 621-629