International Journal of Engineering Research and Development
ISSN: 2278-067X, Volume 1, Issue 2 (May 2012), PP.49-54
www.ijerd.com

Overview on Partial Image Encryption Approaches

Parameshachari B D[1], Panduranga H T[2] , Dr. K M S Soyjaudah[3]
[1]*Department of Electronics & Communication Engg, JSS Academy of Technical Education, Vacoas, Mauritius.*
[2]*Dept. of Electronics, Hemogangothri PG center, University of Mysore, Hassan,Karnataka,India.*
[3]*Department of Electrical & Electronic Engineering, University of Mauritius, Reduit, Mauritius.*

***Abstract*—**Image encryption is vital to ensure confidential transmission and storage of images over internet. However a real-time image encryption is still a challenge due to large amount of data involved. A traditional approach for content access control is to first encode data with a standard compressor and then perform full encryption of the compressed bitstream with a standard cipher (DES, AES, etc.). In this scheme called fully layered, encryptions are totally disjoint process. The limitation of fully layered scheme consists of altering the original bitstream syntax. Therefore, many functionalities of the encoding scheme may be disabled (e.g., scalability). Some recent works explored a new way of securing the content, named partial encryption. Partial image encryption is used to reduce the amount of data to encrypt while achieving a sufficient and inexpensive security. This paper focuses mainly on the different kinds of partial image encryption techniques that are existing, and framing all the techniques together as a literature survey. This study extends to the performance parameters like tunability, visual degradation, compression friendliness, format compliance, encryption ratio, speed, and cryptographic security used in partial image encryption process and analyzing on their security issues.

***Keywords* —**bit stream, format compliance, partial encryption, security, scalability.

I. INTRODUCTION

The high growth in the networking technology leads a common culture for interchanging of the digital images very drastically. Hence it is more vulnerable of duplicating of digital image and redistributed by hackers. Therefore the images has to be protected while transmitting it, Sensitive information like credit cards, banking transactions and social security numbers need to be protected. For this many encryption techniques are existing which are used to avoid the information theft [1]. In recent days of Internet, the encryption of data plays a major role in securing the data in online transmission focuses mainly on its security across the internet. Different encryption techniques are used to protect the confidential data from unauthorized use.

As security is an increasing public concern these days, encryption is becoming popular for any type of sensitive information. An effective encryption scheme that saves the cost and time for data encrypting will be the need of the government, organizations, business companies or individuals. Partial encryption therefore has been proposed for this purpose. In this paper, many of the current important image encryption techniques have been presented and analyzed. An additional feature of partial encryption is to preserve some functionalities of the original bitstream (e.g., scalability). The general approach is to separate the content into two parts. The first part is the public part; it is left unencrypted and made accessible to all users. The second part is the protected part; it is encrypted. Only authorized users have access to *protected part*. One important feature in partial encryption is to make the protected part as small as possible.

Protection against unwanted eavesdropping is essential for the viability of wireless multimedia services. Furthermore, in many wireless applications, network resources, such as bandwidth, and node resources, such as battery power, must be conserved. Since full encryption of transmitted data streams can place a heavy signal processing burden on originating and receiving nodes, one is led to consider the concept of partial encryption of the data streams. In partial encryption only a percentage of the transmitted data stream is processed by an encryption algorithm, with the remainder of the data stream being sent in the clear. The questions to be addressed in partial encryption are: (i) what data must be encrypted to provide the needed level of security? (ii) Can a cryptanalytic attack on the data sent in the clear be mounted that will allow important information about the transmitted data to be discerned by an eavesdropper? (iii) What is the percentage of the data stream that must be protected? Clearly, the data chosen to be protected must be the "most important" bits in terms of reconstruction of the content from the overall data stream, and this idea has lead 'partial encryption'. This paper holds some of those recent existing partial encryption techniques and their security issues.

The rest of the paper is organized as follows: In section 2 we describe performance parameters based on which partial image encryption schemes can be compared or evaluated. In section 3, the performance of all those partial encryption techniques are studied and discussed. In section 4, performance and comparison of these schemes has been given and finally conclusion is drawn in section 5.

II. PERFORMANCE PARAMETERS

We need to define a set of evaluation criteria that will help evaluating and comparing partial image encryption schemes. Some parameters listed below are gathered from literature.

Tunability (T): It could be very desirable to be able to dynamically define the encrypted part and the encryption parameters with respect to different applications and requirements. Static definition of encrypted part and encrypted parameters limits the usability of the scheme to a restricted set of applications.

Visual Degradation (VD): This criterion measures the perceptual distortion of the image data with respect to the plain image. In some applications, it could be desirable to achieve enough visual degradation, so that an attacker would still understand the content but prefer to pay to access the unencrypted content. However, for sensitive data (e.g., military images), high visual degradation could be desirable to completely disguise the visual content.

Compression Friendliness (CF): A Partial encryption scheme is considered compression friendly if it has no or very little impact on data compression efficiency. Some partial encryption schemes impact data compressibility or introduce additional data that is necessary for decryption. It is desirable that size of encrypted data should not increase.

Format Compliance (FC): The encrypted bit stream should be compliant with the compressor. And standard decoder should be able to decode the encrypted bit stream without decryption.

Encryption Ratio (ER): This criterion measures the amount of data to be encrypted. Encryption ratio has to be minimized to reduce computational complexity.

Speed (S): In many real-time applications, it is important that the encryption and decryption algorithms are fast enough to meet real time requirements.

Cryptographic Security (CS): Cryptographic security defines whether encryption scheme is secure against brute force and different plaintext-ciphertext attack? For highly valuable multimedia application, it is really important that the encryption scheme should satisfy cryptographic security. In our analysis we measure cryptographic security in three levels: low, medium and high.

III. RELATED WORK

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.

Cheng and Li,2000 [2] proposed partial encryption methods that are suitable for images compressed with two specific classes of compression algorithms: (a) quadtree compression algorithms, and (b) wavelet compression algorithms based on zerotrees.

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.

H. Cheng and Li, 2002 [3], proposed a novel solution called partial encryption, in which a secure encryption algorithm is used to encrypt only part of compressed data. They proposed partial encryption for quadtree compression. 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

Podesser, Schmidt and Uhl, 2002 [4], 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.

Droogenbroeck and Benedett, 2002 [5] proposed the selective encryption methods for uncompressed (raster) images and compressed (JPEG) image. According to Droogenbroeck and Benedett, at least 4-5 least significant bitplanes should be encrypted to achieve the satisfactory visual degradation of the image.

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.

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.

Zeng and Lei, 2003. [6] Proposed, selective encryption in the frequency domain (8x8 DCT and wavelet domains) is proposed. The general scheme consists of selective scrambling of coefficients by using different primitives (selective bit scrambling, block shuffling, and/or rotation).

A. Wavelet transform case

The proposed scheme combines two primitives.

i) *Selective bit scrambling:* it is a bitplane selective encryption; each individual coefficient bitplane is partitioned into a sign bit, which is very random and uncorrelated with neighboring coefficient sign bits, thus highly unpredictable. Then significance bits (the first nonzero magnitude bit and all subsequent zero bits if any), these give a range for the coefficient value. These bits have lowentropy and thus are highly compressible. Finally, the refinement bits (all remaining bits) are uncorrelated with neighboring coefficients and are randomly distributed. The authors propose to randomly scramble sign bits and refinement bits. The encryption algorithm is not specified.

ii) *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 thatmost 2D local subband statistics are preserved and compression not greatly impacted.

B. DCT transform case

The 8x8 DCT coefficients can be considered as individual local frequency components located at some subband. The same scrambling operations as described above (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 (e.g., a segment can be a slice), 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 are randomly changed and DC coefficients are flipped with respective threshold. 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.

Bergeron and Lamy-Bergot, 2005 [7]. A syntax compliant encryption algorithm is proposed for H.264/AVC [30]. Encryption is inserted within the encoder. To achieve syntax compliance, selected compliant codewords are randomly permuted with other compliant codewords. The shift used for permutation is determined by the AES counter. The main

drawback of this scheme is the lack of cryptographic security. Indeed, the security of the encrypted bitstream 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 ciphertext. This bias depends on the key size and the plaintext space size. The proposed scheme does not give precise values for overall encryption ratio. However, it is mentioned that 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.

Grangetto, Magli, and Olmo, 2006 [8]. The basic approach proposed in is a randomization of the arithmetic coder. This is achieved by randomly swapping the most probable symbol (MSP) and least probable symbol (LSP) intervals. Since only the interval magnitude is important for encoding, the compression performance remains unchanged. Both total and selective encryptions are possible by choosing the layers or resolution levels to encrypt. Selective region encryption is made possible since JPEG2000 is a codeblockbased algorithm. To encrypt a region of interest, they have to apply the encryption on the codeblocks contributing to precincts of the region considered. The low security, brute force attack is feasible. Indeed, trying 30 millions random keys will allow retrieving the secret encryption key. Since arithmetic coding is context based, any error will propagate to subsequent contexts and adversely impact probabilities computations.

Engel and Uhl, 2006. In [9], a JPEG2000 lightweight encryption scheme is proposed. Only lower resolutions are compressed with classical dyadic wavelet transform. For higher resolutions, the algorithm relies on a secret transform domain constructed with anisotropic wavelet packets (AWPs). The aim of this proposal is to allow transparent encryption for applications requiring low-resolution preview. Therefore, low resolution is accessible by all users and decodable with any JPEG2000 compliant codec,limited tunability is permitted. Only lightweight encryption is allowed. Indeed, this algorithm does not allow encrypting lower resolutions. It is intended to particular applications with public thumbnail preview. It offers poor error tolerance since any error in the encrypted parameters for generating random AWP would severely impact the decoding of the bitstream.

Yang Ou, Chul Sur, and Kyung Hyune Rhee, 2007 [10], proposed two novel region-based selective encryption schemes for medical imaging. The first scheme is to randomly invert the first two MSBs of ROI coefficients in wavelet transform domain. It can be efficiently implemented and only incurs little compression efficiency overhead, also it can be extended to other motion formats. The second scheme, selective encryption of the compressed Region of Interest (ROI) data, provides a high level security and has no file size changes. Both of them are format backward compatible and have their own advantage so that they are applicable to different medical security imaging systems to satisfy different requirements.

Nidhi S Kulkarni, Balasuramanian and Indra Gupta, 2008 [11], proposed encryption technique reduces intelligent information in an image by scrambling the image first and then changing the pixel values. The scrambling arrangement is done with the help of a random vector and the pixel values are changed by a simple substitution method which adds confusion and diffusion property to encryption technique. The proposed technique has advantage of convenient realization, less computational complexity and better security. The algorithm is suitable for any kind and any size of gray level image. Tunability of this scheme is not specified. High visual degradation can be achieved. It is compression friendly as well as speed is fast. Encryption ratio of this scheme is 100% as all bits are encrypted. Moderate level of security is obtained. There is a scope of improvement to increase security against brute force attack.

Hammed A younis,Turki Y Abdalla and Abdulkareem Y Abdalla,2009 [12], proposed only 6.25%-25% of the original data is encrypted for four different images, resulting in a significant reduction in encryption and decryption time. According to Hammed A younis,Turki Y Abdalla and Abdulkareem Y Abdalla has low computation complexity and keep an unchanged compression ratio, it could be a nice solution for real time image encryption.From the experiments, they conclude that as the number of clusters in the codebook increases, both PSNR value and execution time and CR increase as well and also shows PSNR versus the number of clusters for Lena image using VQ-Permutation-PE, Wavelet based-VQ-Permutation-PE and Wavelet packet-based-VQ-Permutation-PE, respectively. The proposed methods have good security since the keyspace is very large.

Ju-Young Oh, Dong-Il Yang, Ki-Hwan Chon, 2010 [13], proposed to expand the advandced encrytion standard (AES)-Rijndael with five criteria: the first is the compression of plain data, the second is the variable size of the block, the third is the selectable round, the fourth is the optimization of software implementation and the fifth is the selective function of the whole routine. According to Ju-Young Oh, Dong- Il Yang, Ki-Hwan Chon selective encryption scheme achieves a faster execution speed of encryption/decryption. As encryption schemes become more widely used, the concept of hardware and software co-design is also a growing new area of interest. They proposed a novel encryption algorithm called SEA which is selective and improves the AES algorithm.

Loic Dubois, William Puech and Jacques BlancTalon, 2011 [14], proposed a new approach for the SE of video. The error prediction system of H.264/AVC allows encrypting neighbor MBs of a previous encrypted MB indirectly. In SSE-CAVLC, we have added a prediction system of the decoded frame with an implementation of measures which decides whether to encrypt a given MB or not during the entropy encoding. In this way, only the essential MBs are encrypted while keeping a global final PSNR under the predefined threshold. Indeed, this approach allows to encrypt only a small percentage of the bitstream. However, this method needs some additional computations in the H.264/AVC encoder in order to analyze the confidentiality of the current MB. To sum up, SSE-CAVLC is a solution to the key problems which

are data protection and adequate confidentiality. Further, SSECAVLC optimizes the reduction of the encrypted bits in the H.264/AVC bitstream. Their method consists of two main steps, namely, the memory feedback and the quality measure based.

IV. PERFORMANCE COMPARISON OF PARTIAL IMAGE ENCRYPTION SCHEMES

This section presents performance and comparison among image encryption schemes with respect to various parameters as shown in Table 1.

Table 1. Summary of related work with respect to each criterion

Ref	Tunablity	Visual degradation	Compression Friendliness	Format Compliance	Encryption Ratio	Speed	Cryptographic Security
[2],2000	No	Satisfied	Satisfied	No	depending on content	Fast	not satisfied
[3],2002	No	High	Yes	No	depending on content	Fast	Low
[4],2002	No	High	No	Yes	>37.5%	Fast	Medium
[5],2002	Yes	High	Yes	No	50-60%	Fast	Low
[6],2003	No	High	Compression drop <5%	Yes	20%	Fast	Low
[7], 2005	No	High	Yes	Yes	depending on content	Fast	low
[8],2006	Yes	Variable	Yes	Yes	Variable	Fast	low
[9],2006	No	High	No	No	High	Fast	High
[10],2007	Unspecified	Satisfied	Yes	Unspecified	depending on content	Fast	High
[11],2008	Unspecified	High	Yes	Unspecified	100%	Fast	moderate
[12],2009	Unspecified	variable	Yes	Unspecified	6.25% to 25%	Fast	moderate
[13],2010	Unspecified	Satisfied	Yes	Unspecified	>35%	Fast	High
[14],2011	No	High	Yes	Yes	Variable	Fast	High

V. CONCLUSIONS

In this paper, it has been surveyed that the existing works on the partial encryption techniques. We analyze partial encryption schemes with respect to various parameters as shown in Table 1. Those partial encryption techniques are studied and analyzed well to promote the performance of the partial encryption methods also to ensure the security proceedings. To sum up, all the techniques are useful for real-time image encryption. Each technique is unique in its own way, which might be suitable for different applications. We can conclude that none of the schemes mentioned in Table 1, satisfies all performance parameters. So, it is a challenge for a research to design a partial encryption scheme which maintains good tradeoff among tunability, visual degradation, compression friendliness, format compliance, encryption ratio, speed, and cryptographic security. Everyday new partial encryption technique is evolving hence fast and secure conventional partial encryption techniques will always work out with high rate of security.

REFERENCES

[1]. Eduardo Pinheiro, Borko Furht, Daniel Socek, Ahmet M. Eskicioglu.: Fundamentals of Multimedia Encryption Techniques.

[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]. Howard Cheng and Xiaobo Li, "Partial Encryption of Compressed Images and Videos," IEEE Transaction on Signal Processing, Vol. 48, No. 8, August 2002, pp. 2439- 2451.

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

[5]. 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.

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

[7]. 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 (MMSP '05), pp. 1–4, Shanghai, China, October 2005.

[8]. M. Grangetto, E. Magli, and G. Olmo, "Multimedia selective encryption by means of randomized arithmetic coding," IEEE Transactions on Multimedia, vol. 8, no. 5, pp. 905–917, 2006.

[9]. D. Engel and A. Uhl, "Lightweight JPEG2000 encryption with anisotropic wavelet packets," in Proceedings of IEEE International Conference on Multimedia and Expo (ICME '06), pp. 2177–2180, Toronto, Canada, July 2006.

[10]. Yang Ou, Chul Sur, and Kyung Hyune Rhee, Region-Based Selective Encryption for Medical Imaging ,FAW 2007, LNCS 4613, pp. 62–73, 2007. Springer-Verlag Berlin Heidelberg 2007.

[11]. Nidhi S Kulkarni, Balasuramanian and Indra Gupta.: Selective encryption of multimedia images, XXXII National Systems Conference, NSC 2008, December 17-19, 2008.

[12]. Hammed A younis,Turki Y Abdalla and Abdulkareem Y Abdalla.: Vector Quantization Techniques For Partial Encryption of Wavelet Compressed Digital Images,Iraq Journal Electrical and Electronic Engineering,2009.

[13]. Ju-Young Oh, Dong-Il Yang, Ki-Hwan Chon.: A Selective Encryption Algorithm Based on AES for Medical Information, 2010 ,The Korean Society of Medical Informatics

[14]. Loıc Dubois, William Puech and Jacques Blanc-Talon.: "Smart Selective Encryption of CAVLC for H.264/AVC Video" IEEE, 2011.