A Survey based on Designing an Efficient Image Encryption-then-Compression System

Kalyani G. Nimbokar
M.E.1st Year C.S.E.
Jagadambha College Of Engineering and Technology,
Yavatmal,Maharashtra

Milind V.Sarode
Head of Department C.S.E.
Jagdambha college of Engineering & Technology,Yavatmal

Mangesh M.Ghonge
Assistant Professor of C.S.E.
Jagdamba College Of Engineering and Technology,
Yavatmal,Maharashtra

ABSTRACT

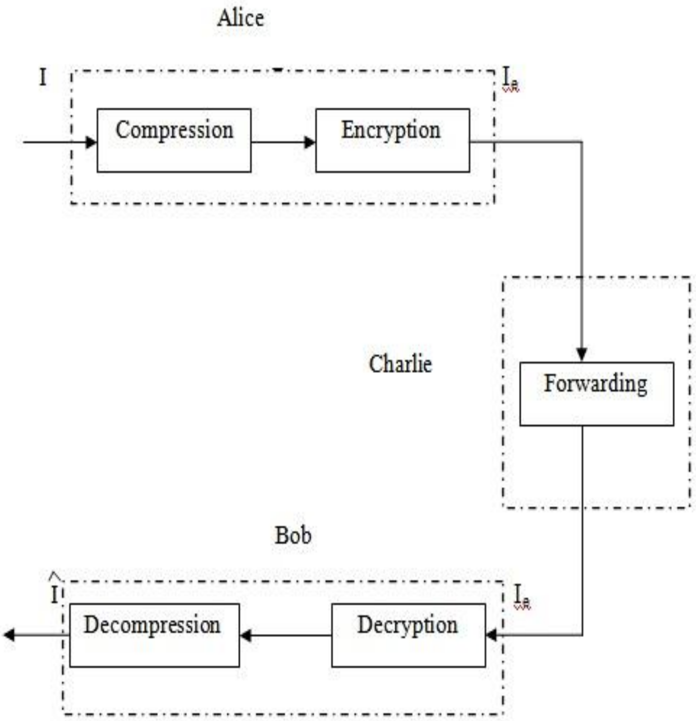
Image encryption has to be conducted prior to image compression. In this paper how to design a pair of image encryption and compression algorithms such that compressing encrypted images can still be efficiently performed. This paper introduced a highly efficient image encryption-then compression (ETC) system. The proposed image encryption scheme operated in the prediction error domain is able to provide a reasonably high level of security**.** More notably, the proposed compression approach applied to encrypted images is only slightly worse, unencrypted images as inputs. In contrast, most of the existing ETC solutions induce significant penalty on the compression efficiency.

Keywords

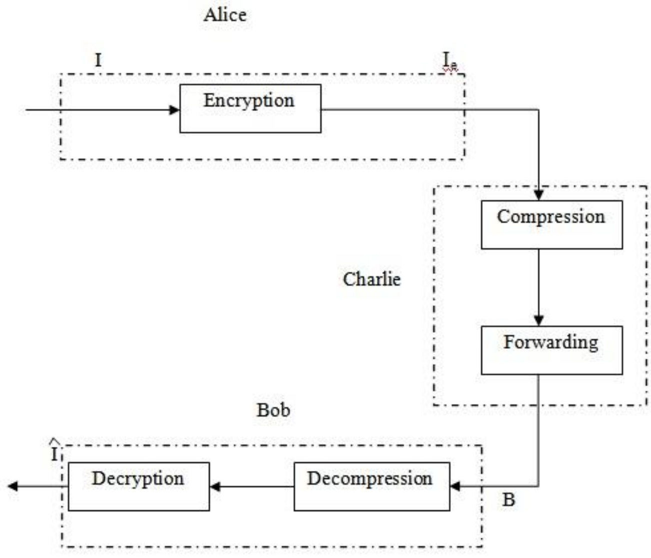
Compression of encrypted image, encrypted domain signal processing

INTRODUCTION

Consider an application scenario in which a content owner Alice wants to securely and efficiently transmit an image *I* to a recipient Bob, via an untrusted channel provider Charlie. Conventionally, this could be done as follows. Alice first compresses *I* into *B*, and then encrypts *B* into *Ie* using an encryption function *EK (·)*, where *K* denotes the secret key as illustrated in Fig.1 (a). The encrypted data *Ie* is then passed to Charlie, who simply forwards it to Bob.[7] Upon receiving *Ie*, Bob sequentially performs decryption and decompression to get a reconstructed image *I*. Even though the above *Compression-then-Encryption (CTE)* paradigm meets the requirements in many secure transmission scenarios, the order of applying the compression and encryption needs to be reversed in some other situations. As the content owner, Alice is always interested in protecting the privacy of the image data through encryption. Nevertheless, Alice has no incentive to compress her data, and hence, will not use her limited computational resources to run a compression algorithm before encrypting the data. This is especially true when Alice uses a resource-deprived mobile device. In contrast, the channel provider Charlie has an overriding interest in compressing all the network traffic so as to maximize the network utilization. It is therefore much desired if the compression task can be delegated by Charlie, who typically has abundant computational resources.A big challenge within such *Encryption-then-Compression (ETC)[7]* framework is that compression has to be conducted in the encrypted domain, as Charlie does not access to the secret key *K*. This type of ETC system is demonstrated in Fig.1 (b).



(a)



(b)

Fig 1:(a) Traditional Compression-then-Encryption (CTE) system; (b) Encryption-then-Compression (ETC) system.

RELATED WORK

The possibility of processing encrypted signals directly in the encrypted domain has been receiving increasing attention in recent years. At the first glance, it seems to be infeasible for Charlie to compress the encrypted data, since no signal structure can be exploited to enable a traditional compressor. Although counter-intuitive, Johnson *et. al* showed that the stream cipher encrypted data is compressible through the use of coding with side information principles, without compromising either the compression efficiency or the information-theoretic security. In addition to the theoretical findings, 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 . By applying LDPC codes in various bit-planes and exploiting the inter/intra correlation, Lazzeretti and Barni presented several methods for lossless compression of encrypted grayscale/color images. Furthermore, Kumar and Makur applied the approach of to the prediction error domain and achieved better lossless compression performance on the encrypted grayscale/color images. Furthermore[1], Zhang designed an image encryption scheme via pixel-domain permutation, and demonstrated that the encrypted file can be efficiently[5],[6] compressed by discarding the excessively rough and fine information of coefficients in the transform domain. Recently, Zhang *et. al* suggested a new compression approach for encrypted images through multi-layer decomposition. Extensions to blind compression of encrypted videos were developed in Despite extensive efforts in recent years, the existing ETC systems still fall significantly short in the compression performance, compared with the state-of-the-art lossless/lossy[7] image and video coders that require unencrypted inputs. The primary focus of this work is on the practical design of a pair of image encryption and compression schemes, in such a way that compressing the encrypted images is *almost* equally efficient as compressing their original, unencrypted counterparts. Meanwhile, reasonably high level of security needs to be ensured. If not otherwise specified, 8-bit grayscale images are assumed. Both lossless and lossy compression [7]of encrypted images will be considered. Specifically, we propose a permutation-based image encryption approach conducted over the prediction error domain

THE ETC SYSTEM

This system includes, the details of the three key components in proposed ETC system, namely, image encryption conducted by Alice, image compression conducted by Charlie, and the sequential decryption and decompression conducted by Bob. Encryption refers to set of algorithms, which are used to convert the plain text to code or the unreadable form of text, and provides privacy. To decrypt the text the receiver uses the "key" for the encrypted text. [7] It has been the old method of securing the data, which is very important for the military and the government operations. Now it has stepped into the civilian‟s day-to-day life too. The online transactions of banks, the data transfer via networks, exchange of vital personal information etc. that requires the application of encryption for security reasons. The feasibility of lossless compression of encrypted images has been recently demonstrated by relying on the analogy with source coding with side information at the decoder. However previous works only addressed the compression of bilevel images, namely sparse black and white images, with asymmetric probabilities of black and white pixels. Upon receiving the compressed and encrypted bit stream B, Bob aims to recover the original image *I* . a multimedia technology for information hiding which provides the authentication and copyright protection.

SECURITY ANALYSIS

This section includes , the analysis regarding the security of the proposed permutation-based image encryption method and the efficiency of compressing the encrypted data. The technique involves three different phases in the encryption process.(fig .2) [8]The first phase is the image encryption where the image is split into blocks and these blocks are permutated. Further permutation is applied based on a random number to strengthen the encryption. The second phase is the key generation phase, where the values used in the encryption process are used to build a key. The third phase is the identification process which involves the numbering of the shares that are generated from the secret image. These shares and the key are then transferred to the receiver. The receiver takes the help of the key to construct the secret image in the decryption process. The technique proposed is a unique one from the others in a way that the key is generated with valid information about the values used in the encryption process. Most of the encryption processes first generate the key and then do the encryption process. This technique generates a relation between the encryption process and the key.[8]

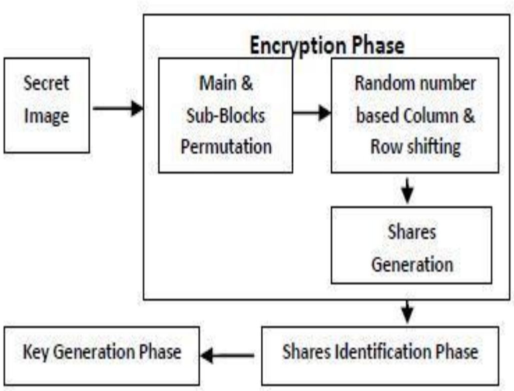

Encryption Phase
Secret Image
Main & Sub-Blocks Permutation
Random number based Column & Row shifting
Shares Generation
Key Generation Phase
Shares Identification Phase

Fig.2 Image Encryption Process

CONCLUSION:

In this paper ,the study of how to design a pair of image encryption and compression technique such that compressing encrypted images can still be efficiently performed. The ETC (Encryption then compression) and CTE (compression then Encryption). we have designed an efficient image Encryption-then-Compression (ETC) system. Within framework, the image encryption has been achieved via random permutation. The analysis regarding the security of the proposed permutation-based image encryption method and the efficiency of compressing the encrypted data.

REFERENCES:

[1] A. Kumar and A. Makur, "Distributed source coding based encryption and lossless compression of gray scale and color images," in *Proc. MMSP*, 2008, pp. 760–764.

[2] D. Schonberg, S. C. Draper, and K. Ramchandran, "On blind compression of encrypted correlated data approaching the source entropy rate," in *Proc. 43rd Annu. Allerton Conf.*, 2005, pp. 1–3.

[3] Z. Erkin, T. Veugen, T. Toft, and R. L. Lagendijk, "Generating private recommendations efficiently using homomorphic encryption and data packing," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 3, pp. 1053–1066, Jun. 2012

[4] T. Bianchi, A. Piva, and M. Barni, "On the implementation of the discrete Fourier transform in the encrypted domain," *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 1, pp. 86–97, Mar. 2009.

[5] X. Zhang, "Lossy compression and iterative recobstruction for encrypted image," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 1, pp. 53–58 Mar. 2011

[6] 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.

[7] Jiantao Zhou, *Member, IEEE*, Xianming Liu, *Member, IEEE*, Oscar C. Au, *Fellow, IEEE*,

[8] and Yuan Yan Tang, *Fellow, IEEE"* Designing an Efficient Image Encryption-Then Compression System via Prediction

[9] Error Clustering and Random Permutation" IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 1, JANUARY 2014.

[10] Sesha Pallavi Indrakanti Associate professor Department of Computer Applications, GVP Degree College (A),Visakhapatnam."Permutation Based Image Encryption Technique*" International Journal of Computer Applications (0975 – 8887) Volume 28– No.8, August 2011*