International Journal of Soft Computing 7 (4): 164-168, 2012
ISSN: 1816-9503

An Innovative Approach of RPC for Secure Transmission of Encrypted Gray Scale Images

Shenbagarajan Anantharajan, P. Subbalakshmi and C. Balasubramanian
Department of CSE, P.S.R. Rengasamy College of Engineering For Women,
Appayanaickenpatti, Sivakasi, Tamilnadu, India

Abstract: Secure transmission over an insecure channel can be achieved through the compression of data for efficiency followed by encrypting it for security. By reversing the operations, it is possible to improve secrecy. The lossless compression of encrypted sources can be achieved through Slepian-Wolf coding. The use of markov properties in the Slepian-Wolf decoder do not work well for grayscale images. This drawback can be rectified by Resolution Progressive Compression (RPC) scheme which compresses the encrypted image progressively in resolution such that the decoder can observe a low resolution version of image, study the local statistics based on it and use statistics to decode the next resolution level.

Key words: Compression of encrypted images, resolution progressive compression, Slepian-Wolf coding, secure, decoder

INTRODUCTION

Conventionally in secure transmission of redundant data as shown in Fig. 1a, the data is usually first compressed and then encrypted at the sender side; to recover the data at the receiver side, decryption is performed prior to decompression. However, in some application scenarios, this conventional diagram needs to be revisited. Let us consider the following case (Fig. 1b). Suppose Alice needs to send information to Bob while Charlie is the network provider (Stallings, 2003). Alice wants to keep the information confidential to Charlie however, the resources that she has is too limited to perform compression. So, Alice just encrypts the data using a simple cipher and gets it forwarded. Charlie as the network provider, always has the interest to reduce the data rate. That is, it is desirable for Charlie to perform compression without having access to the secret key. Johnson *et al*. (2004) prove that in this case, if stream cipher is used by Alice and Bob holds the secret key and performs joint decryption and decompression, the overall system performance can be as good as the conventional approach. That is neither the security nor the compression efficiency will be sacrificed by performing compression in the encrypted domain.

Slepian-Wolf coding, the compression efficiency of the cipher text can be just as good as compressing the plaintext. On the other hand, very good practical Slepian-Wolf codes have been found recently that can approach the theoretical bound for ideal sources, e.g. (Garcia-Frias and Zhao, 2001; Aaron and Girod, 2002, 2005; Bajcsy and Mitran, 2001; Liveris *et al*., 2002; Xiong *et al*., 2004).

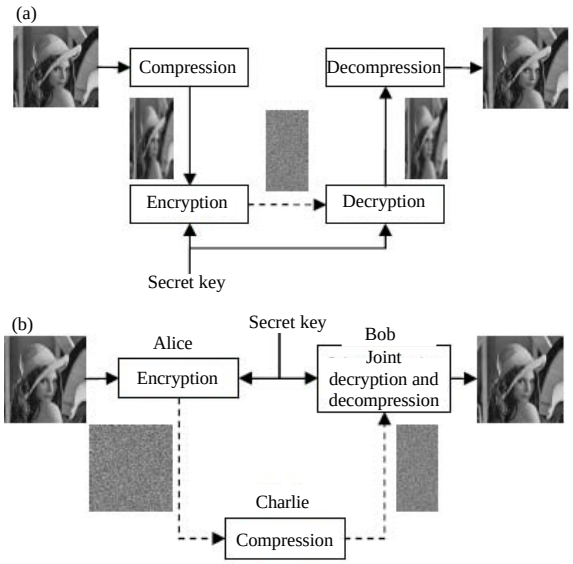

Fig. 1: Secured transmission of redundant data using; a) The conventional approach in which data is first compressed and then encrypted and b) Compression of encrypted data. Solid arrows represent secured channels and dashed arrows denote public channels

Corresponding Author: Shenbagarajan Anantharajan, Department of CSE, P.S.R. Rengasamy College of Engineering For Women, Appayanaickenpatti, Sivakasi, Tamilnadu, India

Lui *et al*. (2010) propose an efficient way to compress encrypted images through Resolution-Progressive Compression (RPC). The encoder starts by sending a down sampled version of the cipher text. At the decoder, the corresponding low-resolution image is decoded and decrypted from which a higher-resolution image is obtained by intra-frame prediction. The predicted image, together with the secret encryption key is used as the Side Information (SI) to decode the next resolution level. This process is iterated until the whole image is decoded. By doing so, the task of de-correlating the pixels which is not possible for the encoder is shifted to the decoder side. In addition by having access to a lower-resolution image, the decoder is able to learn the local statistics, doing much better than blind decoding. Moreover by avoiding exploiting the Markovian property in Slepian-Wolf decoding, the decoder's complexity is significantly reduced.

SURVEY ANALYSIS

The problem of transmitting redundant data over an insecure, bandwidth-constrained communications channel. It is desirable to both compress and encrypt the data. The traditional way to do this is to first compress the data to strip it of its redundancy followed by encryption of the compressed bit stream. The source is first compressed to its entropy rate using a standard source coder. Then, the compressed source is encrypted using one of the many widely available encryption technologies. At the receiver, decryption is performed first followed by decompression. The novelty of reversing the order of older method is to overcome the drawback of traditional method for acquiring secure transmission (Johnson *et al*., 2004). The compressor does not have access to the cryptographic key so, it must be able to compress the encrypted data (also called cipher text) without any knowledge of the original source. A significant compression ratio can be achieved if compression is performed after encryption. This is true for both lossless and lossy compression. The case of lossless compression, researchers use the Slepian-Wolf theorem (Slepian and Wolf, 1973) to show that we can achieve the same compression gain as if we had compressed the original, unencrypted source. For the case of lossy compression, the Wyner-Ziv theorem dictates the compression gains that can be achieved. Here at first we use distributed source coding technique (Pradhan and Ramchandran, 2003).

In the later part of the blind compression technique encryption is followed by compression without compromising either the compression efficiency or the information-theoretic security (Schonenberg *et al*., 2005). This reversal of order is indeed possible in some settings of interest without loss of either optimal coding efficiency or perfect secrecy. The commonly used algorithm for this method of compression is slepian wolf coding. This algorithm it does not focus on the local statistics of the compressed image for the next level, this algorithm does not work well for gray scale images. This algorithm has several drawbacks (Lui *et al*., 2010) such as Slepian-Wolf decoder is expensive, especially in dealing with sources with non-binary alphabets; second, bit-plane based Markov decoding certainly reduces the complexity but the source dependency that originally defined in symbol domain is usually not fully utilized when translated to bit-planes; third since, image and video data are known to be highly non-stationary, a global Markov Model cannot describe its local statistics precisely. To overcome this researchers go for the resolution progressive compression algorithm (Liu *et al*., 2008) here, the encoder starts by sending a down sampled version of the cipher text. At the decoder, the corresponding low resolution image is decoded and decrypted from which a higher resolution image is obtained by interpolation. The interpolated image, together with the secret encryption key is used as the SI to decode the next resolution level. This process is iterated until the whole image is decoded. By doing so, the task of de-correlating the pixels which is not possible for the encoder is shifted to the decoder side. By accessing the low resolution image, the decoder is able to learn the local statistics, doing much better than blind decoding. Moreover by avoiding exploiting the Markovian property in the SWC, the complexity is significantly reduced.

Image compression has been an important research topic for many years. There are many kinds of compression techniques but most of these do not fully take advantage of the characteristics of a target application. In order to transmit redundant data over an insecure and bandwidth-constrained channel (Yang *et al*., 2007) the standard solution is to first compress the data to its entropy rate and then encrypt the result. Here it is investigated that the possibility of reversing the order of these steps, i.e., first encrypting and then compressing without compromising either the compression efficiency or the security. For this purpose there are several algorithms for compressing purpose namely JPEG, Fractal, Spatial and mainly Slepian-Wolf Coding. However, challenges still remain when it comes to practical applications. Considering real-world sources such as images or videos which are typically highly correlated, a critical issue in improving the coding efficiency is how to exploit the source dependency.

Conventional encoder-side decorrelation methods such as transform or prediction are not applicable here because the encryption function has masked the source dependency. In the literature, solutions have been proposed to treat image and video data as Markov sources and to exploit the Markovian property in the Slepian-Wolf decoder (Johnson *et al*., 2004; Schonberg, 2007). A similar research is also found in for non-encrypted colored sources. Some good results have been reported for binary images. However, there are some limitations with this approach: first, Markov decoding in a Slepian-Wolf decoder is expensive, especially in dealing with sources with non-binary alphabets; second, bit-plane based Markov decoding certainly reduces the complexity but the source dependency that originally defined in the symbol domain is usually not fully utilized when translated to bit-planes; third since, image and video data are known to be highly non-stationary, a global Markov model cannot describe its local statistics precisely.

PROPOSED SYSTEM

In this research the secured transmission can be done by encrypting the image and then compressing it. Here this can be done using Resolution Progressive Compression scheme. In this encryption can be done by DES algorithm of encryption, the purpose of encrypting here is to make a secure transmission. The encrypted key will be known only to the encrypter and the decrypter and decompressor not to the compressor. Here decoder and decompressor have been jointly performed to avoid the leack of datas. Then after encyption compression will be carried over using RPC algorithm.

Resolution progressive compression: The compression can be achieved by 2 modules namely, image decomposition and context adaptive interpolation.

Image decomposition: The encoder gets the cipher text Y and decomposes it into four sub-images, namely, the 00, 01, 10 and 11 sub-images. Each sub-image is a down sampled-by-two version of the encrypted image. The name of a sub-image denotes the horizontal and vertical offsets of the down sampling. The 00 sub-image is further down sampled to create multiple resolution levels. Researchers use 00n to represent the 00 sub-image in the n-th resolution level. The 00n sub-image can be losslessly synthesized from the 00n+1, 01n+1, 10n+1 and 11n+1 sub-images. An example of the decomposition is shown in Fig. 2. Here the image is supposed to be an encrypted one. Researchers show it in plaintext just for a better illustration. Meanwhile, researchers would like to point out that the stream cipher function in (1) only scrambles

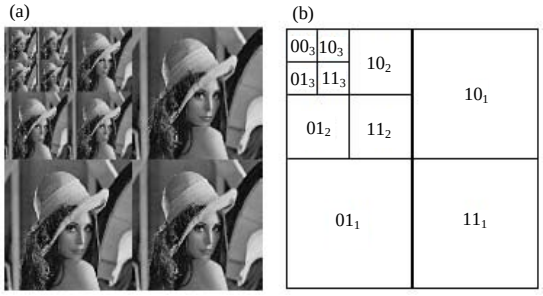

Fig. 2: a) A three-level decomposition of the unencrypted lena image and b) Layout of the sub-images

the pixel values but does not shuffle the pixel locations. This means geometric information of the pixels is still preserved which is leveraged by the down sampling operation.

After the down sampling, each sub-image is encoded independently using Slepian-Wolf codes and the resulting syndrome bits are transmitted from the lowest resolution to the highest. Decoding starts from the 00 sub-image of the lowest-resolution level, say, level N. Researchers suggest transmitting the uncompressed 00N sub-image as the doped bits (Schonberg, 2007). Thus, the 00N sub-image can be known by the decoder without ambiguity and knowledge about the local statistics will be derived based on it. Next, other sub-images of the same resolution level are interpolated from the decrypted 00*N*sub-image. Researchers call the interpolation result the SI of the plaintext. It will then be scrambled the same way as in (1) to generate the SI of the cipher text. Since, it is a one to one mapping between SI of the plaintext and SI of the cipher text for the sake of clarity, researchers use SI only for the former in the rest of the study. Meanwhile, a channel estimation module is employed to estimate the conditional probability density function (pdf) of the original pixel values, given the SI. The SI, the estimated pdf and the corresponding part of the key stream are fed into the Slepian-Wolf decoding module to decode the target sub-image (Fig. 3). When the 01, 10 and 11N sub-images are all decoded and decrypted, the 00N-1 sub-image can be synthesized, then the decoding iterates until the full-resolution image is reconstructed.

Context adaptive interpolation: The SI generation in the scheme is through interpolation. For the sake of simplicity for any pixel in the target sub-image, researchers only use the 4 horizontal and vertical neighbors or the 4 diagonal neighbors in the known sub-image (s) for the interpolation. Intuitively, the SI quality will be better if the neighbors are geometrically closer to the pixel to be interpolated. Hence, researchers use a two-step

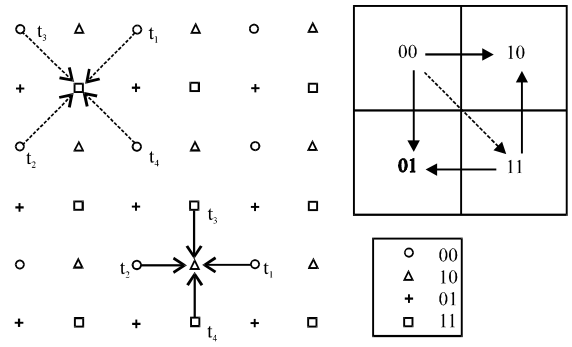

Fig. 3: Two-step interpolation at the decoder side. The dashed arrows denotes the first step interpolation and the solid arrows denotes the second step

Fig. 4: The localized channel estimation. The conditional variance of a pixel in the 10n sub-image is refered to its neighbours in the 10_{n+1} sub-image

interpolation in each resolution level to improve the SI estimation. First, sub-image 11 is interpolated from sub-image 00; after sub-image 11 is decoded, researchers use both 00 and 11 to interpolate 01 and 10. The interpolation pattern is shown in Fig. 4 from which researchers can see another benefit of the two-step interpolation. This two step interpolation simplifies the interpolator design.

Real-world image data is highly non-stationary hence, it is desired to have the interpolation adapted to the local context. For example for a pixel on an edge, it is preferable to interpolate along the edge orientation. Similar efforts can be found in conventional lossless image compression where the Median Edge Detector (MED) and the Gradient Adaptive Predictor (GAP) (Schonberg, 2007) are two successful context adaptive predictors.

However, they process the pixels in a raster-scanning order, thus cannot be directly applied to the scheme. In this subsection, a simple, yet effective Context Adaptive Interpolator (CAI) is proposed for our scheme. Due to the isomorphism, researchers only describe the horizontal-vertical interpolator shown in Fig. 4. Let's be the pixel value to be interpolated, t = [t1, t2, t3, t4]T be the vector of neighboring pixels. The interpolator classifies the local region into four types: smooth, horizontally-edged, vertically-edged and other. In smooth regions, a mean filter is applied; in horizontally/vertically edged regions, the interpolation is done along the edge; otherwise researchers use a median filter. More specifically, the proposed CAI is formulated as:

$$\hat{s} = \begin{cases} \text{mean}(t) & (\max(t) - \min(t) \le 20) \\ (t_1 + t_2)/2 & (|t_3 - t_4| - |t_1 - t_2| > 20) \\ (t_3 + t_4)/2 & (|t_1 - t_2| - |t_3 - t_4| > 20) \\ \text{median}(t) & (\text{otherwise}) \end{cases} \quad (1)$$

In Eq. 1 it can be verified that the first condition contradicts both the second and the third conditions thus a smooth region will never be estimated as edged again. The second and the third conditions are adapted from GAP with an ad hoc threshold. It is also possible that the region is diagonally-edged but there is no clue about on which side of the edge s lies. Therefore, researchers simply adopt a median filter in this case.

Joint decompression and decryption

Localized channel estimation: Slepian-Wolf decoding treats the SI as a noisy version of the source to be decoded. Researchers can consider that there is a virtual channel between the source and the SI (Zixiang *et al*., 2004). To perform Slepian-Wolf decoding, it is n also necessary for the decoder to estimate the statistics of the virtualchannel. In this research, researchers adopt similar settings as in and model the conditional pdf of a pixels to be Laplacian, centered at the given SI ˆs:

$$p(s|\hat{s}) = \frac{\alpha}{2}\exp(-\alpha|s - \hat{s}|) \quad (2)$$

where α and is the variance of p (s $\hat{s}$). Hence, it is necessary for the channel estimator to estimate. Due to the non-stationarity of image data, the accuracy of the SI could vary a lot in different areas. Generally at smooth areas will be much smaller than that at textured areas. Therefore, it is desirable to have a localized channel estimator.

In this research is estimated from the neighboring prediction (interpolation) residual of the previously decoded level. As in this study, Let s be a pixel in the 10n sub-image, the channel estimator observes several geometrical neighbors of s in the 10n+1 sub-image. The neighborhood is chosen to be a 5×5 window. The Mean Square Error (MSE) of the CAI results for these pixels is

scaled to be used as. The scaling is needed because for interpolation at higher-resolution levels, the correlation between the neighboring pixels is higher which usually means smaller prediction residual. It can be seen that both the CAI and the localized channel estimation are based on the assumption that the decoder has access to a lower-resolution reconstruction of the image. In other words, they are both enabled by the resolution-progressive decoding.

CONCLUSION

The secure transmission in an insecure channel can be achieved in this research by first encrypting the image followed by compression. Here the image data undergoes stream-cipher based encryption before compression. Researchers propose resolution progressive compression for this problem which has been shown to have much better coding and compression efficiency and less computational complexity than existing approaches. In this RPC approach joint decompression and decryption is performed to make a data secure. By using RPC the decoder side can learn the local statistics and can produce the better resolution as the original image. The future research will focus on compression of encrypted videos where RPC can be used for both inter-frame and intra-frame correlation learning at the decoder side.

REFERENCES

Aaron, A. and B. Girod, 2002. Compression with side information using turbo codes. Proceedings of the Data Compression Conference, April 2-4, 2002, Snowbird, UT, pp: 252-261.

Aaron, V.A. and B. Girod, 2005. Rate-adaptive distributed source coding using low-density parity-check codes. Proceedings of the Asilomar Conference on Signals, Systems and Computers, November 2005, Pacific Grove, CA, USA., pp: 1203-1207.

Bajcsy, J. and P. Mitran, 2001. Coding for the Slepian-Wolf problem with turbo codes. Proceedinges of the IEEE Global Telecommunications Conference, Volume: 2, November 25-29, 2001, San Antonio, TX, USA., pp: 1400-1404.

Garcia-Frias, J. and Y. Zhao, 2001. Compression of correlated binary sources using turbo codes. IEEE Commun. Lett., 5: 417-419.

Johnson, M., P. Ishwar, V. Prabhakaran, D. Schonberg and K. Ramchandran, 2004. On compressing encrypted data. IEEE Trans. Signal Process., 52: 2992-3006.

Liu, W., W. Zeng, L. Dong and Q. Yao, 2008. Resolution-progressive compression of encrypted grayscale images. Proceedings of the International Conference on Image Processing, October 12-15, 2008, San Diego, California, USA., pp: 2208-2211.

Liveris, A.D., Z. Xiong and C.N. Georghiades, 2002. Compression of binary sources with side information at the decoder using LDPC codes. IEEE Commun. Lett., 6: 440-442.

Lui, W., W. Zeng, L. Dong and Q. Yao, 2010. Efficient compression of encrypted gray scale image. IEEE Trans. Image Process., 19: 1097-1102.

Pradhan, S. and K. Ramchandran, 2003. Distributed source coding using syndromes (DISCUS): Design and construction. IEEE Trans. Inform. Theory, 49: 626-643.

Schonberg, D.H., 2007. Practical distributed source coding and its application to the compression of encrypted data. Ph.D. Thesis, University of California, Berkeley, CA, USA.

Schonenberg, D., S.C. Draper and K. Ramchandran, 2005. On blind compression of encrypted data approaching the source entropy rate. Proceedings of the 43rd Annual Allerton Conference on Communication, Control and Computing, September 28-30, 2005, Monticello, IL, USA.

Slepian, D. and J.K. Wolf, 1973. Noiseless encoding of correlated information sources. IEEE Trans. Inform. Theory, 19: 471-480.

Stallings, W., 2003. Cryptography and Network Security Principles and Practice. 3rd Edn., Prentice-Hall of India Pvt. Ltd., India.

Yang, Y., V. Stankovic and Z. Xiong, 2007. Image encryption and data hiding: Duality and code designs. Proceedings of the IEEE Information Theory Workshop, September 2-6, 2007, Sunnyside-Tahoe City, CA, USA., pp: 295-300.

Zixiang, X., A.D. Liveris and S. Cheng, 2004. Distributed source coding for sensor networks. IEEE Signal Process. Maga., 21: 80-94.