

SMOOTHING AND OPTIMAL COMPRESSION OF ENCRYPTED GRAY SCALE IMAGES

P.S.Kishore^{*}, N.Ajay Nagendra^{*}, K.Pratap Reddy^{*}, V.V.S.Murthy^{**}

^{*} (Student Scholar, Department of ECE, K L University, Guntur, AP, India)

^{**} (Associate Professor, Department of ECE, K L University, Guntur, AP, India)

ABSTRACT

Compression efficiency of encrypted real-world sources such as images can be improved by exploiting source dependency. Lossless compression of encrypted images can be achieved through Slepian-Wolf coding. In this correspondence, we propose a resolution progressive compression scheme which compresses an encrypted image progressively in resolution, such that the decoder can observe a low-resolution version of the image, study local statistics based on it, and use the statistics to decode the next resolution level. Good performance is observed both theoretically and experimentally. We deploy smoothing for images at the receiver to mitigate noise.

Index Terms—compression of encrypted images, Slepian-Wolf coding, resolution progressive compression.

INTRODUCTION:

Government, military and private business amass great deal of confidential images about their patient (in Hospitals), geographical areas (in research), enemy positions (in defense) product, financial-status. Most of this information is now collected and stored on electronic computers and transmitted across network to other computer, if these confidential images about enemy positions, patient, and geographical areas fall into the wrong hands, than such a breach of security could lead to lost of war, wrong treatment etc. Protecting confidential images is an ethical and legal requirement. We store information in computer system in the form of files. File

is considered as a basic entity for keeping the information. Therefore the problem of securing image data or information on computer system can be defined as the problem of securing file data. It is world wide accepted fact that securing file data is very important, in today's computing environment. Good encryption makes a source look completely random, traditional algorithms are unable to compress encrypted data. For this reason, traditional systems make sure to compress before they encrypt. We are using the concept of public key encryption, for the encryption and decryption of image. In this public key's of sender and receiver is known to both but private key's are kept secret. Neither the security nor the compression efficiency will be sacrificed by performing compression in the encrypted domain.

$$Y = X \oplus K. (Y \text{ cipher-text, } X \text{ plain text})$$

where \oplus denotes the bit-wise exclusive OR operation, and K is the key stream.

By employing Slepian-Wolf coding, the compression efficiency of the cipher text can be just as good as compressing the plaintext. 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

EXISTING METHOD:

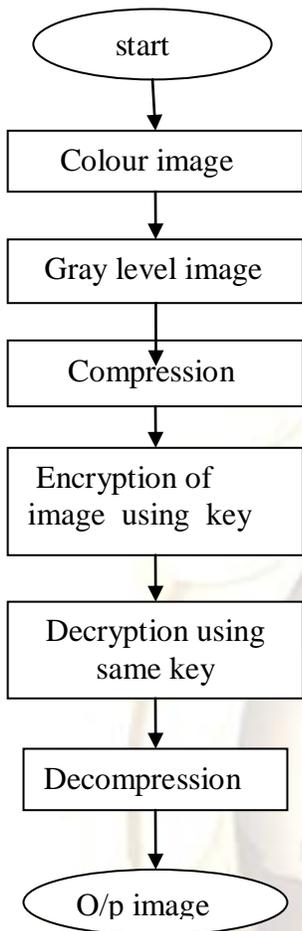


Fig1:data is usually first compressed and then encrypted at the sender side; to recover the data at the receiver side, decryption is performed prior to decompression.

DEPLOYED METHOD:

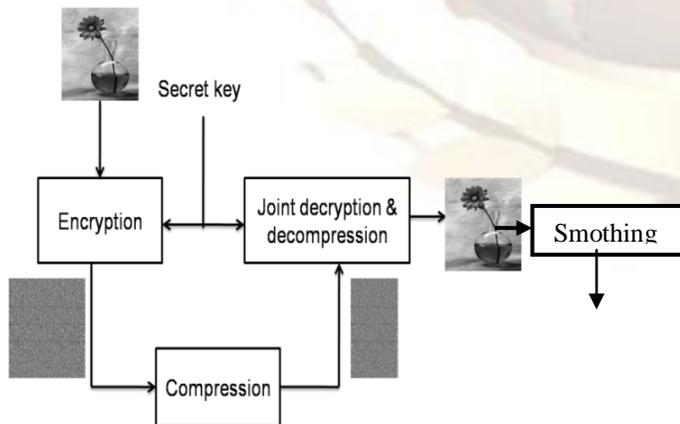


Fig2:The data is encrypted first and the compressed then jointly decrypted and decompressed at receiver

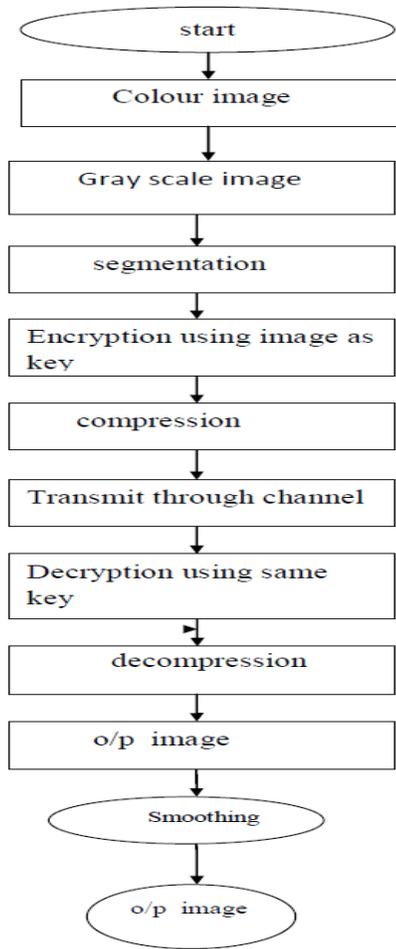


Fig3: flowchart



Fig:4 Illustration of a three-level decomposition of the unencrypted “Lena” image;

SLEPIAN WOLF CODING & DECODING:

The Slepian-Wolf theorem deals with the lossless compression of two or more correlated data streams in the best-known variation, each of the correlated streams is encoded separately and the compressed data from all these encoders are jointly decoded by a single decoder as shown in figure-5 for two

correlated streams. Such systems are said to employ Slepian-Wolf coding, which is a form of distributed source coding. Lossless compression means that the source outputs can be constructed from the compression version with arbitrary small error probability by suitable choice of a parameter in the compression scheme

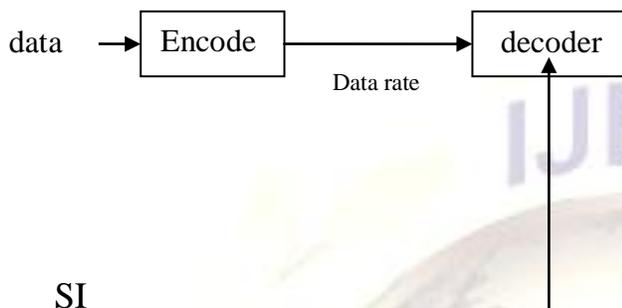


Fig5:slepian-wolf equalent figure

RESOLUTION PROGRESSIVE COMPRESSION OF ENCRYPTED IMAGES:

System Description:

The encoder gets the cipher text Y and decomposes it into several levels. For single-level decomposition, four sub-bands are generated, as illustrated in Figure-4. Each sub-band is a shifted and downsampled-by-2 version of Y , and Y can be losslessly synthesized from the four sub-bands. In fact, it is equivalent to perform a 2-D analysis filter bank on Y , with $H_0(z)=1, H_1(z)=z$. (The corresponding synthesis filter bank is $G_0(z)=1, H_1(z)=z-1$.) We call the four sub-bands as the LL, HL, LH and HH sub-bands, and if multiple-level decomposing is applied, the labels LL_n, HL_n, LH_n and HH_n are used for the sub-bands in the n -th level. The $(n+1)$ th level decomposition is performed on the LL_n sub band. An example of 3-level decomposition of the Lena image is illustrated in Figure4. The encoder encodes each sub-band independently using SWC, and transmits the encoded bits from the lowest resolution to the highest. Decoding starts from the LL sub-band of the lowest resolution level, say, level N . We suggest transmitting the uncompressed LL_n sub band as the doped bits. Thus the LL_n sub band of the image can be known without ambiguity and some knowledge about the local statistics will be derived

based on it. Next, the HHN sub-band is interpolated from LLN. The interpolation result, together with the corresponding part of the key stream, is used as the SI to decode HHN. If this SI is a good approximation of HHN, HHN can be considered as conditionally independent of each other, given the SI. In this case it is not necessary for the Slepian-Wolf decoder to exploit the Markovian property of the source, which reduces the complexity significantly then Slepian-Wolf decoded. Next LL_{n-1} is synthesized and the decoding for level $(N-1)$ is carried out. This process is iterated until the whole image is decoded. It is worth noting that a feedback channel is needed for the encoder to know how many bits to transmit for each sub-band, which generally increases the transmission delay. However, this cost is reasonable because the decoder has no idea about the source statistics at the very beginning, and has to learn it gradually during the decoding. For the sake of simplicity, for any pixel s in the current sub-band, we only use the 4 nearest neighbors (t_1, t_2, t_3, t_4) in the known sub-band(s) for the interpolation, as illustrated in Figure. The reason that we use a 2-step interpolation in level is to improve the quality of the SI. Another reason is that the interpolation patterns in the two steps are isomorphic up to a scaling factor of 2 and a rotation of $\pi/4$.

Context Adaptive Interpolation

The SI generation in our scheme is through interpolation. For the sake of simplicity for any pixel in the target sub-image, we only use the '4' horizontal and vertical neighbors or the '4' diagonal neighbors in the known sub-image(s) for the interpolation.

RESULTS:

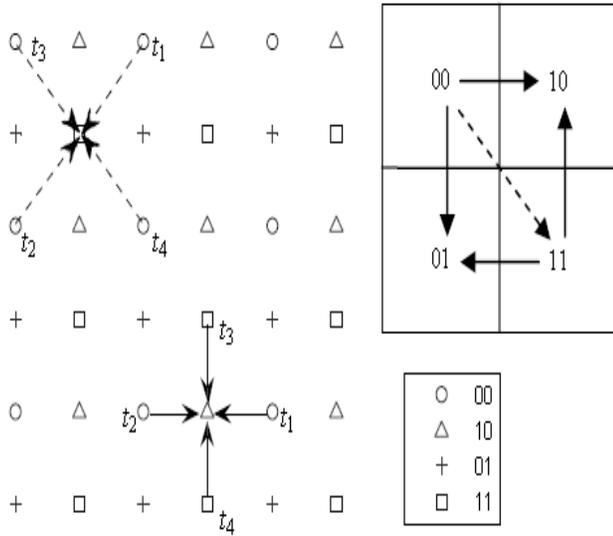
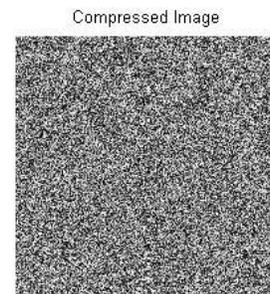
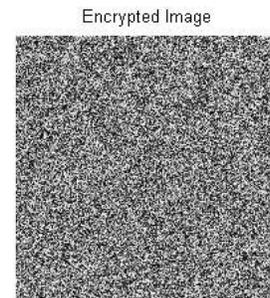
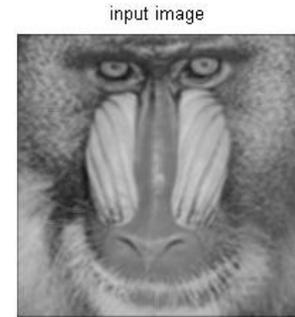
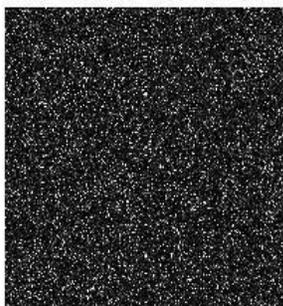


Fig 6: Illustration of the two-step interpolation at the decoder side. The dashed arrows denote the first step interpolation, and the solid arrows denote the second step.

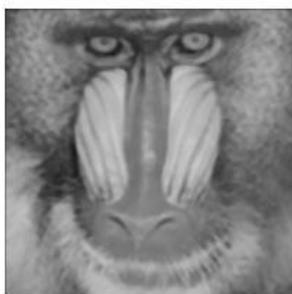
Intuitively, the SI quality will be better, if the neighbors are geometrically closer to the pixel to be interpolated. Hence we use a two-step interpolation in each resolution level to improve the SI estimation. First, sub-image 11 is interpolated from sub-image 00; after sub-image 11 is decoded, we use both 00 and 11 to interpolate 01 and 10. The interpolation pattern is illustrated in Fig. 4, from which we can see another benefit of the two-step interpolation: the interpolation patterns of the two steps are isomorphic up to a scaling factor of $\sqrt{2}$ and rotation of $\pi/4$. It simplifies the design Real-world image data is highly non-stationary, hence it is desired to have the interpolation adapted to the local context.



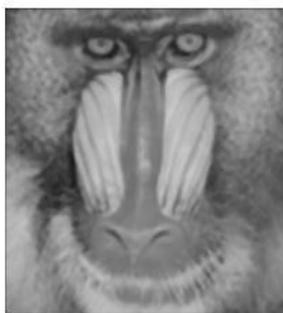
Decrypted Image



retrieved Original Image



filterd Image



In the above results we have shown ,the encryption is done frist in the process so that the data security has been made ,so that the channel cannot estimate what is the data that transmitting .At the receiver's side the decryption is done by providing the SI. Without that key information its impossible to get the original image or data.

CONCLUSION:

In this correspondence, we focus on the design and analysis of a practical lossless image codec, where the image data undergoes stream-cipher based encryption before compression. We deploy resolution progressive compression for this problem. The success of RPC is due to enabling partial access to the current source at the decoder side to improve the decoder's learning of the source statistics. Our future work will focus on compression of encrypted videos, where RPC can be used for both interframe and intraframe correlation learning at the decoder side

FUTURE EXTENSION:

The efficient compression and encryption of images can be performed on videos.

REFERENCES:

- [1] M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, "On compressing encrypted data," *IEEE Trans. Signal Process.*, vol. 52, no. 10, pp. 2992-3006, Oct. 2004.
- [2] W. Stallings, *Cryptography and Network Security: Principles and Practice* (3rd Edition), Englewood Cliffs, NJ: Prentice-Hall, 2003.
- [3] S. S. Pradhan and K. Ramchandran, "Distributed source coding using syndromes (DISCUS)," *IEEE Trans. Inf. Theory*, vol. 49, no. 3, pp. 626-643, Mar. 2003.
- [4] J. D. Slepian and J. K. Wolf, "Noiseless coding of correlated information sources," *IEEE Trans. Inf. Theory*, vol. IT-19, pp. 471-480, Jul. 1973.
- [5] J. García-Frías and Y. Zhao, "Compression of correlated binary sources using turbo codes," *IEEE Commun. Letters*, vol. 5, no. 10, pp. 417-419, Oct. 2001.
- [6] J. Bajcsy and P. Mitran "Coding for the Slepian-Wolf problem with turbo codes," in *Proc. IEEE Global Telecommun. Conf.*, San Antonio, TX. Nov. 2001, pp. 1400-1404.
- [7] A. Aaron and B. Girod, "Compression with side information using turbo codes," in *Proc. IEEE Data Compression Conf.*, Snowbird, UT, Apr.2002, pp. 252-261.
- [8] A. Liveris, Z. Xiong, and C. Georghiades, "Compression of binary sources with side information at the decoder using LDPC codes," *IEEE Commun. Letters*, vol. 6, no. 10, pp. 440-442, Oct. 2002.
- [9] D. Varodayan, A. Aaron, and B. Girod, "Rate-adaptive distributed source coding using low-density parity-check codes", in *Proc. Asilomar Conf. on Signals, Systems and Computers*, Pacific Grove, CA, Nov. 2005, pp. 1203-1207.

- [10] Z. Xiong, A. Liveris, and S. Cheng, "Distributed source coding for sensor networks," *IEEE Signal Process. Mag.*, vol. 21, pp. 80-94, Sep. 2004.
- [11] Y. Yang, V. Stankovic, and Z. Xiong, "Image encryption and data hiding: duality and code designs," in *Proc. Inf. Theory Workshop*, Lake Tahoe, CA, Sep. 2007, pp. 295-300.
- [12] D. Schonberg, *Practical distributed source coding and its application to the compression of encrypted data*, Ph.D dissertation, Univ. of California, Berkeley, CA, 2007.
- [13] D. Varodayan, A. Aaron, and B. Girod, "Exploiting spatial correlation in pixel-domain distributed image compression," in *Proc. Picture Coding Symposium*, Beijing, China, Apr. 2006.
- [14] M. Weinberger, G. Seroussi, and G. Sapiro, "The LOCO-I lossless image compression algorithm: principles and standardization into JPEG-LS", *IEEE Trans. Image Process.*, vol. 9, no. 8, pp. 1309-1324, Aug. 2000.
- [15] X. Wu and N. Memon, "Context-based adaptive lossless image coding," *IEEE Trans. Commun.*, vol. 45, pp. 437-444, Apr. 1997.
- [16] A. Aaron, S. Rane, E. Setton and B. Girod, "Transform-domain Wyner-Ziv codec for video", in *Proc. SPIE Visual Commun. Image Process.*, San Jose, CA, Jan. 2004, pp. 520-528.
- [17] T. Berger, *Rate Distortion Theory: A Mathematical Basis for Data Compression*, Englewood Cliffs, NJ: Prentice-Hall, 1971.
- [18] A. Gersho and R. Gray, *Vector Quantization and Signal Compression*, Boston, MA: Kluwer Academic Publishers, 1992.
- [19] N. Jayant and P. Noll, *Digital Coding of Waveforms: Principles and Applications to Speech and Video*, Englewood Cliffs, NJ: Prentice-Hall, 1984.
- [20] D. N. Rowitch and L. B. Milstein, "On the performance of hybrid FEC/ARQ systems using rate-compatible punctured turbo (RCPT) codes," *IEEE Trans. Commun.*, vol. 48, pp. 948-959, Jun. 2000.
- [21] Q. Yao, W. Zeng, and W. Liu, "Multi-resolution based hybrid spatiotemporal compression of encrypted videos," in *Proc. IEEE Int. Conf. Acous., Speech and Sig. Process.*, Taipei, Taiwan, Apr. 2009, pp.