Simultaneous Encryption/Compression of Images Using Alpha Rooting

Eric Wharton\textsuperscript{1}, Karen Panetta\textsuperscript{1}, and Sos Agaian\textsuperscript{2}

\textsuperscript{1}Tufts University, Dept. of Electrical and Computer Eng., Medford, MA 02155
\textsuperscript{2}The University of Texas at San Antonio, College of Eng., San Antonio, TX 78249

Significant work has been performed on encrypting images and compressing images as two separate problems, but traditional encryption techniques generally degrade the compression ratio. To circumvent these issues, two methods have been used. The first employs known encryption algorithms on compressed image data. The second develops compression algorithms which work well for encrypted data.

Algorithms which encrypt compressed data generally rely on well known encryption methods, such as Digital Encryption Standard (DES) and Advanced Encryption Standard (AES), to encrypt portions of a compressed stream. Also, scrambling methods can be used on JPEG image coefficients to encrypt the image. However, such scrambling techniques have been cryptanalyzed and found to be lacking in security.

Compression of encrypted data can be seen as source coding with side information. To achieve this, a distributed source coding scheme is used whose inter source correlations match the unencrypted source’s statistics. Another method uses an entropy coder to combine run-length and Golomb-Rice encoders to compress Gaussian sources.

The work of Johnson et al. proved that data should be able to be encrypted to the original source entropy regardless of encryption methods. This is based on the assumption that, no matter what, the encrypted data is still related to the original image data with some amount of side information. We develop a novel method to work towards this, using a method which both encrypts the image data and prepares it for compression.

We have shown for a variety of images that we can achieve improved compression ratio using alpha rooting, which has also been used effectively for image enhancement. It functions in the transform domain, reducing the magnitudes of the coefficients while leaving the phase unchanged. We have shown that, by increasing instead of decreasing the magnitudes of the coefficients, an image could be encrypted instead of enhanced. By increasing the relative magnitudes of the coefficients, placing more emphasis on the less important information, a blurred and degraded image is produced. This effect can be reversed by using the same alpha rooting equation and the inverse of the original encryption key.

<table>
<thead>
<tr>
<th>Image</th>
<th>Compression Ratio</th>
<th>MSE(decrypted)</th>
<th>SSIM(decrypted)</th>
<th>SSIM(encrypted)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pentagon</td>
<td>5.4500:1</td>
<td>1.3615x10\textsuperscript{3}</td>
<td>0.5924</td>
<td>1.2708</td>
</tr>
<tr>
<td>Lena</td>
<td>6.0845:1</td>
<td>631.5569</td>
<td>0.8687</td>
<td>1.0795</td>
</tr>
</tbody>
</table>

The contribution of this paper is using alpha rooting to perform simultaneous compression and encryption. This achieves improved compression performance in terms of computational complexity and compression ratio. Results are shown for 2 of the well known benchmark images, using the well known JPEG image compression standard to demonstrate the effectiveness of alpha rooting for simultaneous encryption and compression.