Journal of Artificial Intelligence

ISSN 1994-5450
Why Information Security Demands Transform Domain, Compression and Encryption?

Padmapriya Praveenkumar, K. Thenmozhi, John Bosco Balaguru Rayappan and Rengaranjan Amirtharajan
Department of Electronics and Communication Engineering, School of Electrical and Electronics Engineering, SASTRA University, Thanjavur, Tamil Nadu, India

Corresponding Author: Padmapriya Praveenkumar, Department of Electronics and Communication Engineering, School of Electrical and Electronics Engineering, SASTRA University, Thanjavur, Tamil Nadu, India

ABSTRACT
With the advancement of technology and networking techniques, it is possible to transmit images at a lower bit rate and at the same time with high security. In order to fulfill the security needs of image transmission, several encryption, decryption and image encoding techniques have been put forward. The encryption discussed in this study is the PN (Pseudo Random Number) sequence based encryption using Joint Photographic Experts Group (JPEG) algorithm. In the proposed method, initially the image is portioned into blocks. Run length encoding is done for the level shifted image. Then Discrete Cosine Transform (DCT) and quantization was done and Difference of Quantized DC (DQDC) was calculated. Then the quantized blocks are shuffled based on the PN sequence and then the scrambled images are arranged in zigzag order. Then finally run length and Huffman lossless compression are done to eliminate the additional bits generated using PN codes. Metrics like correlation coefficient, Unified Average Changing Intensity (UACI), Number of Pixels Change Rate (NPCR) were computed to prove the sternness of the proposed method.

Key words: Image encryption, information security, DQDC, PN sequence, UACI, NPCR

INTRODUCTION
With the increase in the usage of networking and internet for the usage of every possible thing, storing and transmission of data in a secured manner has become very inevitable (Praveenkumar et al., 2012a, b, 2013a-d, 2014a-n). Since it is possible for anyone to get an easy access to data, different techniques are used to reduce eavesdropping rate during the transmission. For this, we can use a major combination and collection of the present techniques (Amirtharajan and Rayappan, 2012a-c, 2013; Amirtharajan et al., 2013a-j) like Cryptography, Steganography and Watermarking.

Encryption of data at the transmission end and decryption at the receivers end ensures the safety of our data. Processing of image may not include very sensitive techniques as the change in the pixel contrast will not drastically change the entire message (Praveenkumar et al., 2014a, b; Rajagopalan et al., 2014a, f).

The original data is made unreadable by common man by secret key which helps in encrypting the message called as cipher image. Images convey more information than any written document. With improvement in network techniques, it has become possible to send and receive digital images via wireless communication.
Communication through free space makes it easy for anyone to interpret the transmitted data—wireless communication comes hand in hand with data security techniques (Praveenkumar et al., 2012a, b, 2013a-d, 2014a-n), technically known as information security methods like Cryptography (Praveenkumar et al., 2014a, b; Rajagopalan et al., 2014a-d), Steganography in spatial (Janakiraman et al., 2012, 2013, 2014) or transform domain (Ramalingam et al., 2014a, b; Rajagopalan et al., 2014a-d; Thanikaiselvan et al., 2012a-c, 2013a, b) and watermarking (Amirtharaj and Rayappan, 2013).

One of the security methods followed is the encryption of digital images (Borujeni and Eshghi, 2009; Loukhaoukha et al., 2012; Diaconu and Loukhaoukha, 2013). Carried out at the transmitter, encryption is the process of making the transmitted image unreadable to anyone, except the receiver, using a secret key or algorithm. It plays a vital role and it is maintained as a secret between the transmitter and receiver as anyone with the secret key or algorithm can decrypt the message. The encrypted image is called cipher image.

Encryption can be done by various methods (Borujeni and Eshghi, 2009; Loukhaoukha et al., 2012; Cheddad et al., 2010; Diaconu and Loukhaoukha, 2013; Praveenkumar et al., 2014a, b; Rajagopalan et al., 2014e, f). The most preferred methods are those which consume lesser time without compromising security. After an exhaustive literature survey, this study focuses on PN sequence based encryption along with JPEG and DCT.

MATERIALS AND METHODS

In this technique the working of the signal encryption as given in Fig. 1, goes as follows. The original data is made unreadable by common man by secret key which helps in encrypting the message called as cipher image. Here, PN sequence generation, using JPEG algorithm, is used for making the secret key. The image is divided into 8×8 block then the blocks are level shifted by a level of “2n-1”, where, 2n is the maximum number of gray level.

Then it further undergoes Discrete Cosine Transform (DCT). After this, each block consist of 1 DC and 63 AC coefficients. Then the DC coefficients are quantized and difference between each block is taken and set as the new coefficient except for the first block which remains the same.

Fig. 1: Block diagram of the proposed scheme
Hence, the quantization results are now a relative one. Then the process of Run Length Encoding (RLE) is done to get rid of the zeroes which is a process that converts all the repeating values into a 2 byte value with the first byte contain the number of repetition and the second consists of the value repeated.

Another lossless technique, Huffman coding, can also be used for the same, in which each pixel is provided with a code of variable length. In addition to the JPEG algorithm, scrambling methods are also used to improve NPCR and UACI. This scrambling used can also be split in two-block scrambling (each position of 8×8 block is changed in accordance with PN sequence) and symbol scrambling (each pixel is changed according to the PN sequence generated).

Hence, this method helps us to encrypt the message which can be decrypted by knowing the key algorithm. The difficulty of eavesdropping is directly proportional to the complexity of the key algorithm we prepare. Hence, the data is secured.

RESULTS AND DISCUSSION

In the proposed scheme, 10 test images of size 256×256 were considered and implemented using MATLAB. The computed correlation coefficient, NPCR and UACI were estimated and compared with the available literature as given in Table 1. Figure 2a and b provides the original and level shifted camera man image, respectively.

Figure 3a, b and c denotes the 8×8 DCT terms, quantization matrix of Fig. 3a and the final rounded result of the first 8×8 matrix. Figure 4a and b provides the symbol and the block scrambled images, respectively.

Figure 5a and b provides the final encrypted image and its histogram, respectively. From the histogram it is revealed that uniform distribution of pixels escapes attacks from hackers:

\[
\text{NPCR} = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} A(i,j)}{B \times C} \times 100
\]

Table 1: Computed metrics of the proposed scheme

<table>
<thead>
<tr>
<th>Images</th>
<th>HC</th>
<th>VC</th>
<th>DC</th>
<th>NPCR</th>
<th>UACI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cameraman</td>
<td>-0.0001</td>
<td>-0.0132</td>
<td>-0.0006</td>
<td>99.8647</td>
<td>37.4000</td>
</tr>
<tr>
<td>Peppers</td>
<td>-0.00009</td>
<td>-0.0014</td>
<td>-0.00064</td>
<td>99.7070</td>
<td>26.4711</td>
</tr>
<tr>
<td>Moon</td>
<td>-0.0089</td>
<td>-0.0060</td>
<td>-0.000654</td>
<td>98.8770</td>
<td>24.4031</td>
</tr>
<tr>
<td>Autumn</td>
<td>-0.1210</td>
<td>-0.1675</td>
<td>-0.1479</td>
<td>99.7314</td>
<td>37.6644</td>
</tr>
<tr>
<td>Board</td>
<td>-0.006478</td>
<td>-0.007</td>
<td>-0.01234</td>
<td>99.8779</td>
<td>32.1745</td>
</tr>
<tr>
<td>Shadow</td>
<td>-0.0769</td>
<td>-0.00121</td>
<td>-0.00012</td>
<td>99.9268</td>
<td>36.9001</td>
</tr>
<tr>
<td>Coins</td>
<td>-0.08909</td>
<td>-0.000023</td>
<td>-0.001210</td>
<td>99.8047</td>
<td>33.6236</td>
</tr>
<tr>
<td>Fabric</td>
<td>-0.6712</td>
<td>-0.1865</td>
<td>-0.00002</td>
<td>99.9023</td>
<td>30.9107</td>
</tr>
<tr>
<td>Peers</td>
<td>-0.654</td>
<td>-0.5088</td>
<td>-0.09091</td>
<td>99.9756</td>
<td>34.3795</td>
</tr>
<tr>
<td>Lena proposed</td>
<td>-0.001</td>
<td>-0.0023</td>
<td>-0.00012</td>
<td>99.7666</td>
<td>33.4675</td>
</tr>
<tr>
<td>Lena (Borujeni and Esghii, 2009)</td>
<td>0.005</td>
<td>0.011</td>
<td>0.023</td>
<td>99.7</td>
<td>29.30</td>
</tr>
<tr>
<td>Lena (Loukaouikha et al., 2012)</td>
<td>0.0068</td>
<td>0.0091</td>
<td>0.0063</td>
<td>99.5</td>
<td>28.62</td>
</tr>
<tr>
<td>Lena (Diacono and Loukaouikha, 2013)</td>
<td>0.0002</td>
<td>0.0006</td>
<td>0.0043</td>
<td>99.6</td>
<td>30.50</td>
</tr>
</tbody>
</table>
Fig. 2(a-b): (a) Original cameraman image and (b) Level shifted image of original cameraman

Fig. 3(a-c): (a) 8×8 DCT terms, (b) Quantization matrix of 8×8 DCT and (c) Final rounded result

Fig. 4(a-b): (a) Block scrambled level shifted image of original cameraman and (b) Symbol scrambled block scrambled image of level shifted image of original cameraman
Fig. 5(a-b): (a) Final encrypted image and (b) Histogram of final encrypted image

Fig. 6(a-b): Horizontal distribution of pixel of the, (a) Original image and (b) Encrypted image

where, B, C represents the rows and columns of the original and the encrypted images. If the entire pixel values in the original and the encrypted images are same then $A(i, j) = 0$ otherwise 1:

$$UACI = \frac{\sum_{i=1}^{B} \sum_{j=1}^{C} \text{mod} (x_i(j) - x_{i}(j))}{225} \times \frac{100}{A \times B}$$

where, $x_{i}(i, j)$ and $x_{i}(i, j)$ represents the original and the encrypted images:

$$\text{Correlation coefficient} = \frac{n \sum(xy) - \sum x \sum y}{\sqrt{(n \sum x^2 - (\sum x)^2)(n \sum y^2 - (\sum y)^2)}}$$

where, $n$ denotes the pair of pixels and $x, y$ represents the pixel values in the original and the encrypted images, respectively.

Figure 6a, 7a and 8a provides the pixel distribution along the horizontal, vertical and on diagonal basis of the original cameraman image. Figure 6b, 7b and 8b provides the pixel
Fig. 7(a-b): Vertical distribution of pixel of the, (a) Original image and (b) Encrypted image

Fig. 8(a-b): Diagonal distribution of pixel of the (a) Original image and (b) Encrypted image
distribution along the horizontal, vertical and on diagonal basis of the encrypted cameraman image. From the uniform pixel distribution along the three axes reveals that unknown user cannot gain knowledge about the proposed scheme.

CONCLUSION
In the proposed scheme, encryption algorithm that uses PN sequence along with JPEG and DCT scrambling are utilized to enhance the security of the system multi-fold. Negative correlation coefficient, NPCR of 99.7 and UACI of 38.4 determines the firmness of estimated scheme and found to be better with the available literature. The future study can be extended to colour images and making use of digital watermarking and even can be extended by implementing selective quantization.
REFERENCES


