
Quist-Aphetsi Kester 1,2,3, Laurent Nana1, Anca Christine Pascu1, Sophie Gire1, Jojo M. Eghan3, Nii Narku Quaynor3

1 Lab-STICC (UMR CNRS 6285), European University of Brittany, University of Brest, France
Kester.quist-aphetsi@univ-bret.fr / kquist@ieee.org
2 Faculty of Informatics, Ghana Technology University College
3 Department of Computer Science and Information Technology, University of Cape Coast

Abstract - The growth in multimedia messaging, social networks, live streaming and in other applications have increased overtime. The rise in the engagement of Unmanned Ariel vehicles for agricultural, surveillance and delivery services has become a debate in its security and engagement in today’s cyber physical space. Authentication and security between control units and these devices are of paramount importance. And also a fast and energy efficient algorithms are highly needed to ensure uncompromised situation of computations with these devices. Due to fictitious activities over communication channels by unauthorized users, security and authentication of such transmissions are needed to provide privacy, authentication and confidentiality. In this paper, we proposed a cryptographic encryption technique and a discrete cosine transform for encryption and compression of the transmitted image. We further engaged a frequency domain watermarking approach for the authentication of the digital images. These approaches were engaged to provide several security layers for transmitted image and at the, results showed to be very effective. The implementation in this work was simulated in MATLAB.

Keywords: cryptography, discrete cosine transforms, UAVs, compression, watermarking

1 Introduction

The cyberspace today is challenged with security of transmitted and stored data. The future of computing looks forward to a full potential of sensor networks distributed across the geographical space and yielding a continuous massive data from which knowledge can be deduced from in shaping the way we perceive and adapt to our environment. This will help build and make the physical and the cyberspace be one with each other and resulting into an integrated and interdependent cyber-physical world. One can see these applications gradually evolving from the emergence of new directions in science with restless researchers aiming to get results for complex problems in today’s world. Applications ranging from ubiquitous computing, internet of things, bionics etc. Brain to machine interfacing and brain to brain via device interfacing are gradually progressing in becoming a reality. With all these advancements poses threats to mankind’s security of control. Hence security approaches to securing devices in today’s cyberspace has become key issue in deployment of remote control or Unmanned Ariel Vehicles. These devices first emerge with human autonomy over them and they were gradually given partial independence of autonomous behavior in time. The only interface between these devices and man is the visuals they obtain from afar. These visuals consist of transmitted valuable information such as coordinates, speed, payloads, signal strength etc. Hence a compromise situation or interception of transmitted visuals data can put the vehicle under threat and can expose it to being compromised by a third unauthorized party. And hence the safety and security of the commutations from these devices are key concern. For most of the devices that depend on wireless networks and independent power sources, maximizing cryptographic approaches for them means putting more computational power load on them as well as demanding for more power source and memory for their processes. Hence an effective and efficient and easily implementable but a good layer of security approach is required in providing safety and security for these devices. In contributing to the security developments and demands in these area, we proposed a cryptographic encryption technique to ensure confidentiality and a discrete cosine transform for the compression of the transmitted image. We further engaged a frequency domain watermarking approach for the authentication of the digital images. The paper has the following structure; section II Related works, section III is Methodology, section IV Results and analysis, and section V concluded the paper.
2 Literature Review

The demand for data security for multimedia image applications for use in streaming over secured and unsecured networks has risen over the years. Social network users are in high demand for both security for streaming data and still images in order to counter surveillance activities with the essence of ensuring privacy and security. Applications used for video communications by tech companies are gradually encrypting their streamed data in providing security for their clients. The discrete cosine transform (DCT) is a technique for converting a signal into elementary frequency components and widely used in image compression [1]. There is no so much concern with compression works digital images when there is some tolerance for loss, the compression factor can be greater than no loss tolerance. For this reason, graphic images can be compressed more than text files or programs [2]. PS, A. K. ih their work demonstrated a discrete wavelet technique in compressing the images using wavelet theory in VHDL, Verilog [3]. Xu, N. showed FFT approach for data compression that its histogram has a desired shape [4] and Klimesh, M et al showed the lossless image compression algorithm using FPGA technology [5]. Other works such as Glynn, E. F used Fourier analysis and Image processing technique [6] and Riet, p. shows Image compression Implementation using Fast Fourier Transform [7]. Al-Haj, A. used imperceptible and a robust combined with DWT-DCT digital image watermarking algorithm to provide security for digital images. In their work, they approach engaged used watermarks digital image in combination of the Discrete Wavelet Transform (DWT) and the Discrete Cosine Transform (DCT). His evaluation results show that combining the two transforms improved the performance of the watermarking algorithms that were based solely on the DWT transform [8]. Tomar, Ravi et al in their work showed a robust watermarking technique to copyright an image solely based on Discrete Cosine Transform by embedding blockwise watermark against the noise, filtering and cropping attack. Their experimental results showed that the invisibility and security of the scheme was robust against signal processing [9].

3 Methodology

With our proposed approach, the plain image was encrypted based on the cryptographic approach that involved pixel displacement technique and then compressed before watermarked. Below is a block diagram that illustrates how the entire process engaged. The cryptographic approach is used to conceal the content of the image before the application of the discrete cosine function. The discrete cosine function is then used to compress the image. The watermark is then applied to the compressed image before transmission.

With the proposed system the authentication of the source is verified before decompression takes place. The decompressed image is then decrypted by the approach. But there is an engagement of a symmetric key for the cryptographic process at the earlier phase that is for the image encryption process as well as the later stage which involved the decryption process.

3.1 The Encryption process

- a) Import data from image and create an image graphics object by interpreting each element in a matrix.
- b) Get the size of \( r \) as \([c, p]\)
- c) Get the Entropy of the plain Image
- d) Get the mean of the plain Image
- e) Compute the shared secret from the image
- f) Engage SK for \( g \) to \( q \) using secret key value
- g) Extract the red component as ‘\( r \)’
- h) Extract the green component as ‘\( g \)’
- i) Extract the blue component as ‘\( b \)’
- j) Let \( r = \text{Transpose of } r \)
- k) Let \( g = \text{Transpose of } g \)
- l) Let \( b = \text{Transpose of } b \)
- m) Reshape \( r \) into \((r, c, p)\)
- n) Reshape \( g \) into \((g, c, p)\)
- o) Reshape \( b \) into \((b, c, p)\)
- p) Concatenate the arrays \( r, g, b \) into the same dimension of \( r’ \) or \( g’ \) or \( b’ \) of the original image.
- q) Finally the data will be converted into an image format to get the encrypted image.

The inverse of the algorithm will decrypt the encrypted image back into the plain image.
The secret key is obtained as follows:
\[
Sk = [(c \times p) + (He \times 10^3)] + \left( \bar{x} = \frac{1}{n} \sum_{i=1}^{n} x_i \right) \mod p
\]
Where \( c, p \) are the dimension of the image and \( He \) is the entropy value of the image and \( \bar{x} \) is the arithmetic mean for all the pixels in the image.

### 3.2 The Discrete Cosine Process

DCT transforms a time domain of a signal into its frequency components by only using the real parts of the Discrete Fourier Transform (DFT) coefficients [10]. DCT turns over the image edge to make the image transformed into the form of even function with the character of discrete Fourier transform (DFT) and its inverse manner can be expressed as follows [11]:

The DCT transform of
\[
F(u, v) = \frac{4C(u)C(v)}{n^2} \sum_{j=0}^{n-1} \sum_{k=0}^{n-1} f(j, k) \cos \left( \frac{2j+1}{2n} \right) \cos \left( \frac{2k+1}{2n} \right),
\]

The DCT transform inverse
\[
f(j, k) = \frac{1}{n^2} \sum_{u=0}^{n-1} \sum_{v=0}^{n-1} C(u)C(v) F(u, v) \cos \left( \frac{2j+1}{2n} \right) \cos \left( \frac{2k+1}{2n} \right),
\]

Where \( C(w) = 1/2 \) and when \( w = 0 \) \( C(w) = 1 \) also when \( w = 1, 2, 3, \ldots n - 1 \)

For digital image concept for \( N \)-by-\( N \) image matrix of real numbers we will have [12, 13]

\[
F = \begin{bmatrix}
  f_{00} & f_{01} & \cdots & f_{0(N-1)} \\
  f_{10} & f_{11} & \cdots & f_{1(N-1)} \\
  \vdots & \vdots & \ddots & \vdots \\
  f_{(N-1)0} & f_{(N-1)1} & \cdots & f_{(N-1)(N-1)}
\end{bmatrix}
\]

Where \( f_{ij} \) is pixel value and \( f_{ij}^2 \) is proportional to brightness or energy. Let \( T \) be the transpose vector as follows

\[
\bar{f}_i = (f_{0i}, f_{1i}, \ldots, f_{(N-1)i})^T
\]

The digital image \( F \) can be expressed as formula

\[
F = \begin{bmatrix}
  \bar{f}_0 & \bar{f}_1 & \cdots & \bar{f}_{N-1}
\end{bmatrix}
\]

The engagement of this process was used to compress the image after the image encryption technique.

### 3.3 The watermarking process

Let the host signal defined by \( A \) as below. The following approach was used to embed the data into the image, \( A \). For a given image \( A \), we have

\[
A = \begin{bmatrix}
  x_{11} & x_{12} & \cdots & x_{1n} \\
  x_{21} & x_{22} & \cdots & x_{2n} \\
  \vdots & \vdots & \ddots & \vdots \\
  x_{m1} & x_{m2} & \cdots & x_{mn}
\end{bmatrix}
\]

For a given message \( E \) to be embedded in \( A \) we have,

\[
E = \begin{bmatrix}
  x_{11} & x_{12} & \cdots & x_{1n} \\
  x_{21} & x_{22} & \cdots & x_{2n} \\
  \vdots & \vdots & \ddots & \vdots \\
  x_{m1} & x_{m2} & \cdots & x_{mn}
\end{bmatrix}
\]

Let \( s(R) = \text{size of } R \) be \( [\text{row}, \text{column}] = \text{size of } R = R \times c \times p \) Embedding \( E \) the data into \( A \) will be

\[
d = E_{ij}, \text{ where } d \text{ is the elements of the data to be embedded}
\]

Let the size of \( d \) be \( [c_1, p_1] = \text{size of } d \)

\[
\text{for } i=1:1:c_1 \\
\quad \text{for } j=1:1:p_1 \\
\quad \quad \text{if}(c_1<c) \\
\quad \quad \quad A_{ij} = A_{ij} + E_{ij} \\
\quad \quad \text{else }
\quad \quad \text{end}
\text{end}
\]

The images were encrypted and the results were analyzed below.

### 4 Analysis and Results

The image below was obtained from a Unmanned Ariel vehicle (UAV) was encrypted, compressed, watermarked and analyzed using the proposed approach. The recovery of the plain image from the compressed ciphered image was achieved successfully.

![Figure 2. The plain image from a UAV drone.](image-url)
Figure 3. The ciphered image

Figure 4. The DCT of the ciphered image.

Figure 5. The image of the loss pixel values

Figure 6. The watermarked and compressed image

Figure 7. The IDCT of the dewatermarked and decompressed image

Figure 8. The recovered image from fig 3.

Figure 9. The graph of the normalized cross-correlation of the matrices of the plain image.

Figure 10. The graph of the normalized cross-correlation of the matrices of the ciphered image.

Figure 11. The graph of the normalized cross-correlation of the matrices of the loss pixel values.

Figure 12. The graph of the normalized cross-correlation of the matrices of the watermarked and compressed image.
The normalized cross-correlation of the matrices of is

\[
\gamma(u, v) = \frac{\sum_{x,y} [f(x,y) - \overline{f}] [g(x-u, y-v) - \overline{g}]}{\left[\sum_{x,y} [f(x,y) - \overline{f}]^2 \sum_{x,y} [g(x-u, y-v) - \overline{g}]^2\right]^{0.5}}
\]

\(f\) is the mean of the image templates engaged in the process, \(\overline{f}\) is the mean of in the region under the image template, \(\overline{f}_{uv}\) is the mean of \(f(u,v)\) in the region under the image template. At the end of the entire process, the recovered but compressed, decrypted and dewatermarked image still have visual characteristics that makes it not to be visually different from its original one. And the table below is the mean and entropy values of the images in the process.

TABLE 1: ANALYSIS OF PLAIN, CIPHERD, COMPRESSED, DECOMPRESSED AND DECRYPTED IMAGE.

<table>
<thead>
<tr>
<th></th>
<th>Entropy(p)</th>
<th>Arithmetic mean(m)</th>
</tr>
</thead>
<tbody>
<tr>
<td>PI</td>
<td>7.1726</td>
<td>125.8161</td>
</tr>
<tr>
<td>EI</td>
<td>7.1726</td>
<td>125.8161</td>
</tr>
<tr>
<td>CI</td>
<td>1.1960</td>
<td>5.7262</td>
</tr>
<tr>
<td>WCI</td>
<td>0.4492</td>
<td>94.7262</td>
</tr>
<tr>
<td>ICI</td>
<td>7.1753</td>
<td>125.8147</td>
</tr>
<tr>
<td>LI</td>
<td>2.0720</td>
<td>1.1645</td>
</tr>
<tr>
<td>DI</td>
<td>7.1753</td>
<td>125.8147</td>
</tr>
</tbody>
</table>

PI=plain image, EI= Encrypted Image, CI=Compressed Image, WCI=Watermarked and Compressed Image, ICI=Decompressed and dewatermarked Image, LI= Image Loss due to compression, DI=Decrypted Compressed Image

5 Conclusion

Our proposed approach was resistant against statistical and brute force attacks. The encryption process was effective for all the images and there was no pixel expansion at the end of the process. But there was an effective loss of pixel value during the encryption process but it was insignificant to the visuals of the image. The entropy and mean values for the images in were computed and indicated in the table above. The total entropy and the mean of the plain images never changed for all the ciphered images and that of the dewatermarked and the recovered images also remained the same.

Acknowledgments. This work was supported by Lab-STICC (UMR CNRS 6285) at UBO France, AWBC Canada, Ambassade de France-Institut Français-Ghana and the DCSTIT-UCC, and also Dominique Sotteau (formerly directeur de recherche, Centre national de la recherche scientifique (CNRS) in France and head of international relations, Institut national de recherche en informatique et automatique, INRIA) and currently the Scientific counselor of AWBC.

References