
Sowmya D & Tejaswini S
Assistant Professor Department of CSE JNNCE, Shivamogga, Karnataka, India
Department of CSE JNNCE, Shivamogga, Karnataka, India

Abstract: Digital multimedia which can be transmitted over computer network is prone to security issues hence high security and privacy is important. Combined approach of cryptography and steganography is achieved. Blowfish encryption algorithm is combined with K-means color clustering technique is used to accomplish image security.

I. Introduction

The data security has gotten to be a standout among the huge issues in data communication. So it turns into a conjoined some portion of data communication. With a specific end goal to address this issue, cryptography [1] and can be consolidated with steganography. Cryptography and steganographic techniques are combined to achieve image security goals.

Cryptography, planning a secured communications and it is reasonable only to the individual having a key. It implies both to decrypting secret writing and to the utilization of codes to change over modernized information so that lone a particular beneficiary will have the capacity to perceive it utilizing a key.

Cryptography can be routinely utilized to supplant or in blend with steganography [2]. Before, it guaranteed mystery in communication. Cryptography is dispatched in to two different ways. They are,

- More than keeping secrets it makes use of computerized signature.
- It is helpful for figuring and information transfers and clients are not aware of it.

Blowfish encryption algorithm is used for procedure of encryption. Colour based image steganography is used to hide secret image into cover image. It performs different operations on both sender side as well as receiver side. Colour based image steganography uses clustering method and pattern matching method. Cryptography joined with steganography gives better image security. Many symmetric key cryptographic algorithms [3] perform differently and blowfish algorithm is preferred.

1. Blowfish Encryption algorithm

Blowfish is very strong algorithm none of the attack is sustained against it. Blowfish Algorithm [4] makes use of feistel Network, emphasizing straightforward encryption16 times. It consists of 64 bit block size, and key length varies from 32-bits to 448 –bits.

Algorithm 1: Blowfish Encryption Algorithm

1. The input is a 64-bit data element, x.
2. Divide x into two 32-bit halves: xL, xR.
3. Then, for i = 1 to 16:
4. xL = xL XOR Pi
5. xR = F(xL) XOR xR
6. Swap xL and xR
7. After the sixteenth round, swap xL and xR again to undo the last swap.
8. Then, xR = xR XOR P17 and xL = xL XOR P18.
9. Finally, recombine xL and xR to get the cipher text.

1.1 Generating Sub-Keys:

Blowfish uses a substantial number of sub-keys. These keys must be pre-forms before any information encryption takes place. Figure 1 illustrates generation of subkeys using blowfish algorithm.

- The P-exhibit includes 18 different 32-bit subkeys. P1, P2,..., P18.
- It contains 4 S-boxes which is of 32-bit each and involves 256 entries for each of the boxes.

\[ S_{1,0}, S_{1,1},..., S_{1,255} \]
\[ S_{2,0}, S_{2,1},..., S_{2,255} \]
\[ S_{3,0}, S_{3,1},..., S_{3,255} \]
\[ S_{4,0}, S_{4,1},..., S_{4,255} \]

Imperial Journal of Interdisciplinary Research (IJIR)  Page 1674
Fig. 1: S-box

**Step 1:** Initially P-exhibit later different S-boxes of fixed length is considered together. The string comprises of the hexadecimal digits of pi: $P_1 = 0x243f6a88$, $P_2 = 0x85a308d3$, $P_3 = 0x13198a2e$, $P_4 = 0x03707344$, and so forth.

**Step 2:** $P_1$ is xor’d with 32 bits of the key, $P_2$ is xor’d with the 2nd 32-bits of the key and so on continues up to $P_{14}$. Iteration continues until all the p-exhibit is xor’d with keys.

**Step 3:** Encoding is done with blowfish algorithm, utilizing the sub keys.

**Step 4:** Supplant $P_1$ and $P_2$ along with product obtained from step 3.

**Step 5:** Output of step 3 is used and encrypted using altered keys.

**Step 6:** Supplant $P_1$, $P_2$ along with results of step 3.

**Step 7:** Proceed with the procedure, supplanting all entries of the P array, and afterward every one of the 4 S-boxes, with the yield of the industriously changing Blowfish algorithm.

### 1.2 Feistel Network

Feistel system is a technique for changing function typically called as function $F$, it is a block cipher. This structure involves preferences of encryption and decryption process both operations are very similar that is not possible to distinguish. In some cases just have to reverse the keys. Feistel systems is product cipher, thus consolidate numerous rounds of rehashed operations for example,

- Bit-rearranging, this is referred as permutation boxes that are P box.
- Non-straight functions are used called as substitution boxes S Box.
- Modular algebra using XOR function for linear blending.

The Feistel System works as,

- Each block is divided into two equal parts.
- Right half turns out to be left half.

- New right part is obtained by XORing the left part along with results of $f$ function to key and right part.
- Previous rounds are inferred regardless of possibility that capacity $f$ is not invertible.

Construction of feistel networks follows some of the steps and iterative operations. The basic operations are,

- Plaintext block is divided into two equal halves, left part (L0), right part (R0).
- For every round, $i$ value from 1 to $n$ computations are done as given by equations 3.1 and 3.2.

$$L_i = R_{i-1}$$

$$R_i = f(R_{i-1}, K_{i-1})$$

Where round function is $f$ and sub-key is depicted as $k_i$.

- Decryption is accomplished as given by equation 3.3 and 3.4.

$$R_{i-1} = L_i$$

$$L_{i-1} = R_i \oplus f(L_i, K_i)$$

### 2. Cluster Based Image Steganography

Embedding process utilizes hybrid steganographic technique which incorporates color clustering [5] and pattern matching strategies. Along with clusters different patterns of different color are generated. These distinctive groups contain diverse number of pixels. The clusters with biggest number of pixels are chosen to insert secret information.

Clusters are made of group of similar color pixels. The articles are fundamentally the same as each other in a group and exceptional with objects of various bunches. The procedure of grouping similar pixels is known as clustering. Clusters can be distinguished based on colors pallets, size of pixels and so on. One of the important character of cluster is it holds useful information. That valuable information gets distinctive inside the cluster. This methodology is utilized as a part of image steganography.

Clusters are created by using pattern matching methods. The items which are comparable in shading are gathered in a cluster. In pattern matching, a color palette is utilized for examination of color with pixel color. Pattern matching method utilizes k-means algorithm.

#### 2.1 K-means Algorithm

This technique is computationally proficient and can be connected to multidimensional information. K-means [6] is an iterative strategy that is utilized to segment a picture into k-groups. Figure 2 specifies flow of k-means algorithm. The essential method in k-means algorithm is as following.
The dataset is apportioned into K bunches and the information is focused randomly on to the clusters, resulting clusters have approximately have same number of information focuses.

For every information point:
- Calculate the separation from the information point to every cluster.
- If the information point is nearest to its own particular group, abandon it where it is. In the event that the information point is not nearest to its own cluster, move it into the nearest cluster.

Re-process the cluster focus by averaging the majority of the pixels in the cluster.

Repeat steps 2 and 3 until merging is accomplished.

II. Experiment and Result

As the secret image has been implanted in the clusters of cover image, the visual distortion may present in the secret image implantation that can't be seen by the human eye. Keeping this in mind the main goal is to assess visual distortions presented by the embedding process. The quality metric picked is the Peak to Signal Ration (PSNR), Mean Square Error (MSE) and Elapsed Time (ET). PSNR is communicated in decibels (dB). The secret image is implanted by keeping up a proper balance in the middle of strength and imperceptibility.

Table 1 shows comparison of the values of the quality metrics such as PSNR, MSE and ET values are calculated for different test data. Quality metrics is measured between cover image and secret image obtained in proposed algorithms, after embedding the secret image S1, S2, S3 and S4 in the corresponding Cover image C1, C2, C3 and C4. Different test data is considered and apply quality measure on each of the image. PSNR, MSE, ET values are calculated for each spread picture and stego picture is considered in the table 1 and values of corresponding images are tabulated in the table 2.

Graphs are plotted for quality metrics such as PSNR, MSE and ET values which are tested on different dataset. Figure 3(a), (b) and (c) specifies the comparison metrics with respect to different images based on PSNR values, MSE values and ET values correspondingly.

Fig. 2: K-means

Fig. 3: Clustering using k-means algorithm
Table -1 Data Set

Table -2 Experiment Results

<table>
<thead>
<tr>
<th>Host Image</th>
<th>Quality Metric</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1,S1</td>
<td>PSNR</td>
<td>50.748</td>
</tr>
<tr>
<td></td>
<td>MSE</td>
<td>0.5516</td>
</tr>
<tr>
<td></td>
<td>ET</td>
<td>5.7</td>
</tr>
<tr>
<td>C2,S2</td>
<td>PSNR</td>
<td>50.820</td>
</tr>
<tr>
<td></td>
<td>MSE</td>
<td>0.5516</td>
</tr>
<tr>
<td></td>
<td>ET</td>
<td>5.87</td>
</tr>
<tr>
<td>C3,S3</td>
<td>PSNR</td>
<td>50.75</td>
</tr>
<tr>
<td></td>
<td>MSE</td>
<td>0.5516</td>
</tr>
<tr>
<td></td>
<td>ET</td>
<td>5.57</td>
</tr>
<tr>
<td>C4,S4</td>
<td>PSNR</td>
<td>50.50</td>
</tr>
<tr>
<td></td>
<td>MSE</td>
<td>55.16</td>
</tr>
<tr>
<td></td>
<td>ET</td>
<td>5.726</td>
</tr>
</tbody>
</table>

Fig. 3: Comparison of metrics with respect to different images (a) PSNR (b) MSE (c) ET

III. CONCLUSION

A combined approach of cryptography and steganography is utilized as a part of request to guarantee abnormal state of security during transmission over communication channel. Strong
blowfish encryption algorithm is used along with cluster based image steganography which enhances high chance of security. Framework adds up with an advantage of color image clustering. The picture quality has been measured utilizing different execution parameters like Peak sign to commotion proportion (PSNR), Elapsed Time (ET) and mean square mistake (MES).

IV. REFERENCE