PIP (Picture In PICTURE) against image theft using ICE algorithm

A. Agnes Ahalya \(^1\) and J. Janet Silviya\(^2\)

Abstract
With the increased usage of social media, digital data like images are more prone to unauthorized download, image theft, and other similar attacks. To overcome this stenography and encryption techniques are used where steganography hides the original image under a pseudo image and the symmetric encryption converts the image into an unreadable form. This paper describes about designing of new algorithm using Picture in Picture (PIP) steganography, Inverse theorem of differentiable functions and Function composition. In this algorithm, the inverse theorem is used to generate a composite key using an image and a mathematical function and the function composition is used to encrypt the original image using the uploader key. The algorithm also includes quadrant repositioning technique and for enhanced encryption, a shared secret key is used which undergoes \([K^\ast KT]\) transformation which is followed by a dynamic modulo transposition module and XOR encryption of the image bytes using the forward reverse approach. The new algorithm designed includes both steganography and encryption techniques to enhance integrity and confidentiality.

Keywords
Function composition, Forward reverse approach, Inverse theorem, Modulo transposition, PIP steganography, quadrant repositioning, shared secret key.

AMS Subject Classification
68U10.

1,2 Loyola ICAM College of Engineering and Technology, Chennai, India.
*Corresponding author: 1 agnesahalya.20cs@licet.ac.in; 2 janetsilviya.20cs@licet.ac.in
Article History: Received 10 January 2020; Accepted 01 May 2020

1. Introduction
The images play a major role in social media websites, uploading an image on common platforms like Facebook, Instagram is getting increased over a decade. If not secured anyone can make use of these images without authorization.
The newly designed ICE algorithm helps the uploader to prevent theft of images from their websites. Every existing algorithm functions based on the image properties like color, greyscale and the list continues. [1] describes the combination of steganography and encryption is used where AES has used for encryption and the TIP technique is implemented using LSB algorithm but this is not sufficient for images as image handling is complex than text handling, hence improvisation is required. [2] explores the possibility of using an image as a key. [3],[4] explains the existing key designs for steganography and encryption and their limitations. [5] explores about chaotic theory a significant property in image encryption. [6],[7] introduces about 3 tier architecture. Now a new algorithm was designed which inherit positive factors of previous designs and was named ICE (Inverse theorem, Composition of functions and Encoded matrix).

2. Entities of the algorithm

The algorithm takes into the assumption that for an image uploaded in a website 3 actors are involved

1. Website owner
2. Image owner(may or may not be the website owner)
3. A user who wants to view the image(Maybe website owner or Image owner or a third person) Hence the algorithm is designed to support 3 key encryption architecture fused with enhanced techniques of transposition and basic PIP steganography.

The description of the keys is as follows:

1. A composite key generated from a unique key image and a continuous differentiable mathematical function that is assigned to the website owner. This key follow an asymmetric key mechanism
2. A text key designed by an image uploader
3. A dynamic session key

The techniques used in the algorithm are:

1. Modulo Transposition
2. Quadrant repositioning
3. Forward Reverse Approach

3. Working of the modules

3.1 Website owner key generation

To design the composite of website owner it makes use of inverse theorem of functions.

**Theorem 3.1.** If $f$ is a continuously differentiable function with nonzero derivative at the point $a'$; then $f$ is invertible in a neighborhood of $a'$, the inverse is continuously differentiable, and the derivative of the inverse function at $b = f(a')$ is the reciprocal of the derivative of $f$ at $a'$:

$$f^{-1'}(b) = \frac{1}{f'(a)}$$

3.2 Uploader key generation

The uploader key on encryption undergoes $g_1, f$ transformation and on decryption $f^{-1}, g_2^{-1}$

$$g_1 = mx + c$$
$$g_2 = m(x + c)$$
$$f = x + c.$$  

3.3 Dynamic key generation

Random function is applied in the shared master key

3.4 Modulo transposition logic:

**Encryption:**

- n:Total number of bytes
- d:divisor
- for $i = 0$ to $n-1$
- for $k = 0$ to $d-1$
- for $j = 0$ to $n-1$
- if $j = k$
- $y[j] = x[i]$

**Decryption:**

- n:Total number of bytes
- d:divisor
- for $i = 0$ to $n-1$
- for $k = 0$ to $d-1$
- for $j = 0$ to $n-1$
- if $j = k$
- $x[i] = y[j]$

3.5 Forward Reverse Approach:

The secret image is taken in original order whereas key image is taken in reverse order for encryption.

3.6 Quadrant Repositioning:

The images are divided in 4 quarters are replaced as where first quarter is positioned in third quarter the second quarter in fourth and vice versa.

![Quadrant repositioning](image)

4. ALGORITHM FLOW:

4.1 Encryption Algorithm

4.1.1 Secret Image Encryption using Image owner key
4.1.2 Key Image Encryption using Public key of Website owner

- Acquire Key Image value and function \( B = [b_1, b_2, \ldots, b_k] \), \( f(B) \)
- Compute \( f(B) \) and store it in \([kba]\) array

4.1.3 Transposition and Transformation of bytes

- Quadrant reflection\( (eba) \)
- Design an dynamic third party key for transposition\[ text\]
- Form \([Kt * KtT]\) store it in \([KP]\)
- Sub algo\( (eba) \)
  for \(i > (0ton - 1)\)
  for \(k > (0tod - 1)\)
  for \(j > (0ton - 1)\)
  if \(j == k\)
  \(x[i] = y[j]\)
- Quadrant reflection\( (eba) \)

4.2 Decryption algorithm

- Remove cover

4.2.1 Key Image Encryption using Private key of Website owner

- Acquire Key Image value and function \( A = [a_1, a_2, \ldots, a_k] \), \( f'(A) \)
- Compute \( f'(A) \) and store it in \([kba]\) array

4.2.2 Transposition and Transformation of bytes

- Read encrypted image as byte array\( [eba] \)
- Acquire third party key for transposition \( [Kt] - text\)
- Form \([Kt * KtT]\) store it in \([KP]\) for every \(KP\)
- \([oba]=XOR(eba\ and\ kba)\) forward reverse approach

5. PERFORMANCE METRICS

5.1 Time

The time estimation of encryption and decryption process was done in an i5 processor which is subjected to variation based on processing power (See Table 1 and Table 2).

5.2 Avalanche property

Avalanche (The property wherein slight change in input causes tremendous change in output) is one of the desirable property of any cryptographic algorithm. Ten different images were taken and passed into the ICE algorithm. Fig. 2, Fig. 3, Fig. 4 represents the variations imposed by the corresponding keys in the encrypted image with respect to slight change in their values.

| No. of characters | 1MB | 5MB | 10MB | 20MB |
|-------------------|-----|-----|------|------|
| 2                 | 182 | 288 | 905  | 1279 |
| 4                 | 140 | 250 | 719  | 1301 |
| 8                 | 156 | 263 | 720  | 1246 |
| 16                | 141 | 257 | 686  | 1280 |
| 32                | 156 | 275 | 799  | 1310 |

| No. of characters | 1MB | 5MB | 10MB | 20MB |
|-------------------|-----|-----|------|------|
| 2                 | 131 | 351 | 795  | 1255 |
| 4                 | 286 | 745 | 1946 | 3198 |
| 8                 | 733 | 202 | 5885 | 9710 |
| 16                | 2384| 7399| 20303| 35145|
| 32                | 6613| 20363| 56444| 98893|
Table 1. Time estimation for encryption process in (ms)

Table 2. Time estimation for encryption process in (ms)

Figure 3. Histogram representing the Avalanche property of website owner key.

Figure 4. Histogram representing the Avalanche property.

Figure 5. Histogram representing the Avalanche property of dynamic session key.

5.3 Accuracy
Accuracy is the measure of similarity between the original image and decrypted image.

5.3.1 SSIM: The structural similarity (SSIM) index is a method for predicting the perceived quality of digital images.

5.3.2 PSNR: Peak signal to noise ratio, often abbreviated PSNR, is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity.

5.3.3 CROSS CORRELATION: Cross Correlation is a valid technique to relate provide similarity and best match between two signals.

6. Conclusion
We proposed an algorithm that supports the CIA triad and reduces the complexity of implementation. The given algorithm achieves most of the user requirements but it does...
suffer from few setbacks like increased storage is required, design of key requires a database of possible key functions, a secure channel of key transmission is required and error Correction is not supported. In the future, if this algorithm is appended to credential/access filtering technique this then image theft percentage could be reduced to a considerable extent and possible ECC are being researched that could be used with this algorithm.

**ACKNOWLEDGMENT**

We like to thank Loyola Icam College of Engineering and Technology for their constant support and we would also like to extend our gratitude to Santa Maria Matric. Hr. School for allowing us to test ICE algorithm in their official website.

**References**

[1] Naveen Chandra Gowda, P. Sai Venkata Srivastav, Guru Prashanth.R, Raunak.A, Madhu Priya R., “Steg Crypt (Encryption using steganography), *International Journal of Engineering and Advanced Technology* 8(5s)(2019), 2249-8958.

[2] Madhu Sudan, Vipul sharma, Two New Approaches for Image Steganography Using Cryptography, “Third International Conference on Image Information Processing, 2015; DOI: 10.1109/ICIIP.2015.7414766.

[3] Abdelkader Moumen and Hocine Sissaoui, Images Encryption Method using Steganographic LSB Method, AES and RSA algorithm, *Nonlinear Engineering*, 6(1)(2017), 53–59.

[4] Radha S. Phadte, Rachel Dhanaraj, Enhanced Security with Steganography and Cryptography, *IOSR Journal of Computer Engineering (IOSR-JCE)*, 11-16.

[5] Nath, Asoke and Roy, Sayudh and Gopalika, Chahat and Mitra, Debayan, Image Steganography using Encrypted Message, *International Journal of Advance Research in Computer Science and Management Studies*, 5(4)2017, 1–10.

[6] Sahil Lotlikar, Ashish Gupta, Jayesh Thorat, Sandhya, Image Steganography and Cryptography Using Three Level Password Security, *International Journal for Research in Applied Science & Engineering Technology* 5(IV)(2017), 1–10.

[7] Arshiya Sajid. A, Mohammad Sajid. M, Mohammad Tanvir. P. A Comparative Study of Recent Steganography Techniques for Multiple Image Formats, *International Journal of Computer Network and Information Security*, 11(1)(2019), 11-25.