Reversible Data Hiding in Encrypted Images using Paillier Cryptosystem with Chaotic Maps

Thurimerla Prasanth and Dr. B Geetha Vani
1P.G Scholar, 2Professorprasanth1586@gmail.com, Department of Computer Science and Engineering, Narayana Engineering College, Nellore, Andhra Pradesh, India-524004.

Abstract: Reversible Data hiding in encrypted images is acquiring a special interest in recent years. There exists so many methods to encrypt and decrypt the images. These existing methods are reversible but not lossless. In this paper, we proposed a reversible and lossless data hiding method in encrypted images with the help of shared key along with public and private keys. The plain input image is encrypted using Paillier cryptosystem with shared key and target binary image is encrypted with chaotic maps. Then the binary image is embedded directly into the encrypted plain input image. At the receiver, the data is extracted with the help of shared key. This method is reversible and lossless with infinite PSNR and embedding rate of 1 bpp. The results of the proposed method are found to be effective when compared with other methods in the literature.

Index Terms - Reversible and lossless data hiding in encrypted images; chaotic image encryption; Paillier image encryption; Bogdanov map; Ideal decryption.

I. INTRODUCTION

Image sharing needs to be protected from unauthorized access and attacks from intruders. Sharing images in cloud platform is more prone to attacks like data theft and also there is a chance of using confidential information in illegal activities. Hence a strong cryptosystem is needed to provide authentication, confidentiality, and integrity. Content modification and concatenation during transmission will give better result to provide data privacy up to an extent [1]. Even having zero knowledge about the original plain content and/or key used for encryption, images can be retrieved completely [2].

There are few methods of reversible data hiding in the encrypted domain. This methods have been designed especially for retrieving images with maximum possible clarity and to ensure authentication in encrypted domain [3],[4]. In these methods, we can embed an encrypted message in any image which is already encrypted but no one have complete knowledge about original content and/or key used for encryption. During Decryption, the original image must be fully retrievable and also the encrypted message must be decoded accurately. Hence, Quality of reconstructed image and privacy of embedded message are most important.

More number of Reversible image hiding methods are developed in recent years [5],[6].All these methods are not able to retrieve the image quality as expected in expected levels. So, we are presenting an interesting combination of reversible data hiding with Paillier cryptosystem with Bogdanov map which yielded ideal image reconstructed quality compared to the methods in literature survey.

II. RELATED WORKS

Reversible data hiding methods meets the requirement of authentication and data enrichment. It also embeds a secret message into images after encryption. At the receiver side, the encrypted image and hidden message are extracted with maximum possible quality. This process yields lossless results after image decryption. Histogram shifting [7]-[9] and difference expansion [10], [11] are few good techniques and also some techniques combine both histogram shifting and difference expansion [12],[13].

There are few methods like visual secret sharing [14] which allows to look into the way how the image is encrypted by knowing original image or the key used in encryption time. One more technique which follows the same is recompression of crypto-compressed images [15]. In the methods like reversible data hiding in encrypted images [5] both clear images and shared key kept secret to the user.
The intention behind our proposed scheme is to provide additive homomorphism by using the Paillier cryptosystem [16] for the purpose of reversible data hiding. The main advantage of adapting this cryptosystem is no one has the clear idea about both the original image and the type of key generation. This is possible because of its large key space and the typical random number generation in both encryption and decryption process. The key used in the Bogdanov map is shared to both transmitter and receiver sides for target image transmission and extraction. Along with this shared key, the Paillier cryptosystem provides more security in terms of public and private keys.

The remainder of this paper is designed as follows: Section 3 describes about the proposed methodology of reversible data hiding in encrypted images. The experimental results, discussion and conclusion are presented in Section 4, Section 5 and Section 6 respectively.

3. METHODOLOGY

In this section, the methodology of proposed reversible and lossless data encryption in encrypted images is explained. The Fig.1. illustrates the entire process of our methodology.

A. Paillier cryptosystem

Paillier cryptosystem [16] is one among the decent crypto systems which is a probabilistic asymmetric public key encryption system that follows additive homomorphic property. In this paper, the input image is encrypted using the Paillier encryption method. It consists three steps: key generation, encryption phase, and decryption phase.

(i) Key generation

Let us select two large prime numbers \( u \) and \( v \) such that \( \text{gcd}(uv,(u-1)(v-1)) = 1 \). Let \( n = uv \) and \( \lambda = \text{lcm}(u-1,v-1) \) Then select a integer randomly \( g \) and make sure that \( n \) divides the order of \( g \).

\[
\mu = (H(g^2 \mod n^2))^{-1} \mod n
\]  

(1)

Where \( H(x) = \frac{x-1}{n} \) for any given \( x \). Here \((n, g)\) is the public key used at encryption phase and \((\lambda, \mu)\) is the private key used at the decryption phase.

![Diagram](http://indusedu.org)

Fig. 1. Proposed method for reversible and lossless data encryption in encrypted images.
(ii) Encryption phase

Let \( I(x, y) \) be the input image with \( x \) and \( y \) as coordinate points. Select a random number \( r(x, y) \) such that

\[ 0 \leq r(x, y) \geq n \]

and ensure that \( \gcd(r, n) = 1 \). The cipher image, \( C \) can be computed from the original image, \( I \) as

\[ C(x, y) = g^{i(x,y)r(x,y)n \mod n^2} \]  

(2)

The random number \( r(x, y) \) can be generated using Bogdanov map [17]. It is produced by the interaction of Hamiltonian and dissipative dynamics. This is more complex map in chaotic encryption systems.

The Bogdanov map can be produced by

\[ x_{n+1} = x_n + y_{n+1} \]  

(3)

\[ y_{n+1} = y_n + \epsilon y_n k x_n (x_n - 1) + \mu x_n y_n \]  

(4)

where \( 0 < k < 4, \mu = -0.1, \) and \( \epsilon = 0.0049 \).

The algorithm for decryption is illustrated in algorithm 1.

(iii) Decryption phase

Let \( c \) be the cipher image, then compute the input image, \( I \) as

\[ I'(x, y) = H(c(x,y)^3 \mod n^2) \mu \mod n \]  

(5)

The algorithm for decryption is illustrated in algorithm 2.

B. Chaotic encryption for additional data
The chaotic encryption used for the additional data follows the methodology in [18]. This chaotic encryption is the combined version of logistic [19], Gauss and Henon [20] maps as shown in Fig. 2. The additional data taken here in the form of target image.

(i) Logistic map

The eq. (6) is the equation for Logistic map. It acts as a polynomial mapping with degree two.

\[ x_{k+1} = rx_k(1 - x_k) \]  

(6)

Where \( x_k \) is a number, belongs to(0,1). The better values for the parameter \( r \) lies in the interval [0,4]. many times this method represents a demographic model due to this the logistic map suffers from pathological problem. This problem leads decrease in population sizes to less than zero for some parameter values and few initial conditions. So it is nice to take the value of the parameter \( r \) close to four.

(ii) Gauss map

It is possible to map a surface in Euclidean space to the unit sphere. For this purpose the gauss map in differential geometry is good mapping technique. It can be expressed as,

\[ x_{n+1} = \exp(-ax_n^2) + \beta \]  

(7)

The surface must be oriented to define the Gauss map. In this case the degree matches with half of the Euler characteristic. The value of \( \alpha \) is 4.90 and \( \beta \) is in the range(−1,1).

(iii) Henon map

The Henon map unveils the chaotic behaviour as it is a discrete time dynamical systems. This map is one among the best dynamical systems. Using this map, a new point can be mapped by taking input from a point \((x_t, y_t)\) in the plane.

\[ x_{t+1} = 1 - ax_t^2 + y_t \]  

(8)

\[ y_{t+1} = by_t \]  

(9)

The map hinge on values \( a \) and \( b \). The values \( a = 1.4 \) and \( b = 0.3 \) are the values for classical Henon map. This map exhibits chaotic behaviour for the classical values and for the remaining values the behaviour may be intermittent, chaotic, or sometimes converge to a periodic orbit.

Fig. 2. Encryption of additional data.

C. Data embedding and extraction

The cipher image is added directly to the binary image in data embedding process. But at the receiver, the shared key, \( k \) is used to extract the embedded binary image. The Bogdanov map key is implemented at both
transmitter and receiver for faithful reconstruction of data. The image embedding and extraction are presented in Algorithm 3, 4.

---

Algorithm 3 Binary image embedding to encrypted original image

**Require:** Encrypted image, C and encrypted data image T

**Ensure:** Encrypted image with data C’

1: \([m,n]\leftarrow \text{size}(C)\);
2: for \(i = 1\) to \(m\) do
3:     for \(j = 1\) to \(n\) do
4:         \(C'(i,j)\leftarrow C(i,j)+T(i,j)\);
5:     end for
6: end for
7: return \(C'\)

---

Algorithm 4 Binary image extracting from \(C'\)

**Require:** Encrypted image with data, \(C'\), private key \((\lambda, \mu)\) and shared key \(k\).

**Ensure:** Extract binary image T

1: \([m, n]\leftarrow \text{size}(C')\);
2: Generate \(r(i, j)\) using shared Bogdanov key, \(k\)
3: for \(i = 1\) to \(m\) do
4:     for \(j = 1\) to \(n\) do
5:         \(\text{temp}\leftarrow C'(i, j)\);
6:         for \(G = 0\) to \(255\) do
7:             \(\text{temp1}(ii)\leftarrow g^G r(i, j)^n \mod n^2\);
8:         end for
9:         for \(jj = 0\) to \(255\) do
10:            \(\text{temp2}(ii)\leftarrow \text{dist}(\text{temp},\text{temp1}(jj))\);
11:        end for
12:        \(T(i, j)\leftarrow C'(i, j)-\text{temp1}(\text{find(min(temp2)))};
13:    end for
14: end for
15: return \(C'\)

---

IV. RESULT ANALYSIS

Input image encryption

The input image is encrypted using Paillier Cryptosystem. The input images and their cipher images are shown in Fig. 3. The PSNR (peak signal to noise ratio) and bpp (bit per pixel) are evaluated to validate the proposed model. The PSNR value represented as

\[
PSNR = 10 \log_{10} \frac{255^2}{\sum_{x,y}(I(x,y) - I'(x,y))^2}
\]

Where \(I(x,y)\) is the reconstructed image from cipher image.
TABLE I COMPARISON WITH OTHER METHODS

<table>
<thead>
<tr>
<th></th>
<th>Lena</th>
<th>Baboon</th>
<th>Airplane</th>
</tr>
</thead>
<tbody>
<tr>
<td>Embedding rate</td>
<td>PSNR</td>
<td>Embedding rate</td>
<td>PSNR</td>
</tr>
<tr>
<td>(bpp)</td>
<td>(dB)</td>
<td>(bpp)</td>
<td>(dB)</td>
</tr>
<tr>
<td>[4]</td>
<td>0.5</td>
<td>39.53</td>
<td>0.5</td>
</tr>
<tr>
<td>[8]</td>
<td>0.02</td>
<td>48.2</td>
<td>0.06</td>
</tr>
<tr>
<td>[21]</td>
<td>1</td>
<td>48.67</td>
<td>1</td>
</tr>
<tr>
<td>[22]</td>
<td>0.156</td>
<td>44.65</td>
<td>0.156</td>
</tr>
<tr>
<td>[23]</td>
<td>0.156</td>
<td>inf</td>
<td>0.156</td>
</tr>
<tr>
<td>[5]</td>
<td>0.9681</td>
<td>inf</td>
<td>0.9681</td>
</tr>
<tr>
<td>proposed</td>
<td>1</td>
<td>inf</td>
<td>1</td>
</tr>
</tbody>
</table>

Target image encryption

Completely lossless chaotic encryption is used for the encryption of target image. The images and the corresponding encrypted images are shown in Fig. 4.
V. DISCUSSION

we are compared our proposed method and six classical methods to point the improvement in embedding rate and PSNR. Very recent techniques are proposed by Puteaux et al. [5],[21].In this process we used the popular images of Baboon, Lena and Airplane. The payload in the proposed method is more when compared with other methods in each and every case. In fact, the proposed method is independent of image content. No other techniques give such an immense results in such situations. But the Lena image used in method [23] and the original image is same. Even for the remaining images our proposed scheme has improvement over the other methods.

VI. CONCLUSION

In this work, we proposed a better performing method that allows sharing of confidential images using Paillier cryptosystem based reversible data hiding technique which provides more embedding space. This method performs decently compared with few recent methods.

In future work, we are thinking that increasing the number of bits per pixels in hiding is possible. Just like, transmitting two or three binary target images at an instance of time.

References


