High Security Image Steganography with Modified Arnold’s Cat Map

Minati Mishra  
Fakir Mohan University  
Balasore, India

Ashanta Ranjan Routray  
Fakir Mohan University  
Balasore, India

Sunit Kumar  
J. C. College, Kolhan University, Jharkhand

ABSTRACT

Information security is concerned with maintaining the secrecy, reliability and accessibility of data. The main objective of information security is to protect information and information system from unauthorized access, revelation, disruption, alteration, annihilation and use. This paper uses spatial domain LSB substitution method for information embedding and Arnold’s transform is applied twice in two different phases to ensure security. The system is tested and validated against a series of standard images and the results show that the method is highly secure and provides high data hiding capacity.

General Terms

Digital Image Processing, Steganography, Security

Keywords

Arnold’s cat map, Encryption, Cover image, Decryption

1. INTRODUCTION

Steganography is an art of hiding information in ways that prevent the detection of hidden messages and this is achieved by hiding a piece of information inside another piece of innocent looking information. There exist a number of data embedding methods such as the spatial and time domain methods, Transform domain methods and fractal encoding methods etc. These methods hide/embed information in different types of media such as text, image, audio, video etc. Amongst these varieties of different file formats, digital images are considered to be the most popular type of carriers because of their size and distribution frequency. Covert or hidden communication is the process of hiding a piece of information in another information. There are a number of covert communication techniques such as: Cryptography, Steganography, Covert channel, Anonymity, Watermarking etc [1]. Steganography is one of the effective means of data hiding that protects data from unauthorized or unwanted disclosure. It works by hiding secret messages into ordinary and innocent looking messages those are generally out of suspicion. Digital image Steganography procedures exploit the high capacity and widely used digital images for data hiding purposes.

A digital image is a two dimensional function f(x, y) where, x and y are spatial coordinates, f is the amplitude at (x, y) , also called the intensity or gray level of the image at that point and x, y, f are finite- discrete quantities [2]. Digital Image processing is the use of computer algorithms to perform image processing on digital images. It allows a wider range of complex and sophisticated algorithms to be applied to digital images with ease and with a much effective way in comparison to analog signal processing [3].

Figure 1, depicts the general block diagram of image Steganography where at the transmitter’s end a secret message is embedded to an innocent looking cover image and the resultant stegoimage which is visually same as the original cover is then transmitted over the communication channel without raising any suspicion in the minds of intermediate unintended sniffers/ receivers [4]. At the receiving end the secret message is extracted by the authorized receiver using an extraction algorithm and a valid key. To make this process even more concealed and robust, the message is often encrypted using some encryption technology before embedding and has to be decrypted during extraction to reveal the message.

1. ARNOLD’S CAT MAP

Arnold’s cat map (ACM) or Arnold transform (AT), proposed by Vladimir Arnold in 1960, is a chaotic map [6] which when applied to a digital image randomizes the original organization of its pixels and the image becomes

Figure 1. Block diagram of Steganography System

There exist both spatial as well as transform domain image Steganography methods [5]. The transform domain procedures are more robust and are commonly used for watermarking purposes whereas the spatial domain methods provide higher capacity and are popular for Steganographic use. LSB substitution is a popular spatial domain method that replaces the lower order image bits those do not carry much useful image information by the secret message bits. In this paper we have used a modified Arnold’s Cat Map technique to encrypt the message and the experimental results show that the proposed method provides higher data hiding capacity with improved security and simultaneously preserves the quality of the cover without causing any visual distortion to it.

2. ARNOLD’S CAT MAP

The experimental results show that the method is highly secure and provides high data hiding capacity.
imperceptible or noisy. However, it has a period \( p \) and if iterated \( p \) number of times, the original image reappears.

**Definition:** The generalized form of Arnold’s cat map can be given by the transformation \( \Gamma : \mathbb{T}^2 \rightarrow \mathbb{T}^2 \) such that:

\[
\begin{pmatrix}
    x' \\
    y'
\end{pmatrix} =
\begin{pmatrix}
    2 & 1 \\
    1 & 1
\end{pmatrix}
\begin{pmatrix}
    x \\
    y
\end{pmatrix} \pmod{N} \quad (1)
\]

Where, \( x, y \in \{0, 1, 2 \ldots N -1\} \) and \( N \) is the size of a digital image.

A new image is produced when all the points in an image are manipulated once by equation (1).

Arnold’s Cat Map (ACM) is a simple but powerful transform [7] and digital image encryption can be achieved by applying this in the following manner:

Let \( p \) be the transform period of an \( N \times N \) digital image \( I \). Applying ACM for a random iteration of \( t \) times (\( t \in [1, p] \)) to \( I \), a scrambled image \( \Gamma \) is obtained which is completely chaotic and is different from \( I \). Now \( \Gamma \) can be transmitted over the communication channels without revealing any information to the unauthorized receivers or sniffers [8,9]. At the receiving end the process is repeated for \( (p - t) \) times to obtain back the original image. Figure 2 shows the results of Arnold transformation applied to a gray scale Lena image.

![A. Original Image](image1)

![B. Applying 25 times ACM to A](image2)

![C. 95 times ACM](image3)

Figure 2. Arnold’s Transformation applied to Lena Image

### 3. MODIFIED ARNOLD TRANSFORM

It can easily be seen that the original Arnold transformations given by equation (1) can be modified to produce a sequence of Arnold transformations as given below:

\[
\begin{pmatrix}
    x' \\
    y'
\end{pmatrix} =
\begin{pmatrix}
    i & i + 1 \\
    1 & 1
\end{pmatrix}
\begin{pmatrix}
    x \\
    y
\end{pmatrix} \pmod{N} \quad (2)
\]

OR

\[
\begin{pmatrix}
    x' \\
    y'
\end{pmatrix} =
\begin{pmatrix}
    i + 1 & i \\
    1 & 1
\end{pmatrix}
\begin{pmatrix}
    x \\
    y
\end{pmatrix} \pmod{N} \quad (3)
\]

Where,

\[
i \in \{1, 2, 3 \ldots \}
\]

Transformations given by equations (2) and (3) are periodic as \( \text{abs}(\det(A)) = 1 \) in both the cases where, \( A = [a, b; c, d] \) is the Arnold transform matrix.

Equations (2) and (3), given above, produce a sequence of different Arnold Transforms applied to 128x128 grayscale Lena image.

This demonstrates that there is virtually no overlap in the feature space among the four species to be identified. This means that the classifier will not have to work hard to separate the various species from each other and then to use that information to identify a given feature vector with its associated tree species [13,14]. Here the data are normalized 4000 iterations by using the z-score normalization.

**Figure 3. Periodicity of modified AT for different values of i**

From this above picture, it is clear that:

a) the Arnold periodicity varies between 128, 192 and 252 for different \( i \)-values for the same 128x128 ‘micky’ image when the first pair of equations are used and when the second pair of equations are used there are 5-different Arnold periodicities between 50 to 252 [15].

b) All these transform functions map the image bits differently.

c) Images scrambled with a particular AT cannot be restored using a different AT [16].

The following example demonstrates the above observations:

Let \( I \) be a 3 x 3 matrix given by:

\[
I = [1 \ 2 \ 3; 4 \ 5 \ 6; 7 \ 8 \ 9]
\]
Applying the transformation given in equation (1) to I for 1, 2, 3, 4 numbers of times it can be seen that the periodicity in this case is 4.

\[
A_1 = \begin{bmatrix} 1 & 9 & 5 & 6 & 2 & 7 & 8 & 4 & 3 \end{bmatrix} \\
A_2 = \begin{bmatrix} 1 & 3 & 2 & 7 & 9 & 8 & 4 & 6 & 5 \end{bmatrix} \\
A_3 = \begin{bmatrix} 1 & 5 & 9 & 8 & 3 & 4 & 6 & 7 & 2 \end{bmatrix} \\
A_4 = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{bmatrix}
\]

Whereas transforming I through a modified AT given by equation (3) for i=3, we get:

\[
B_1 = \begin{bmatrix} 1 & 4 & 7 & 8 & 2 & 5 & 6 & 9 & 3 \end{bmatrix} \\
B_2 = \begin{bmatrix} 1 & 8 & 6 & 9 & 4 & 2 & 5 & 3 & 7 \end{bmatrix} \\
B_3 = \begin{bmatrix} 1 & 9 & 5 & 3 & 8 & 4 & 2 & 7 & 6 \end{bmatrix} \\
B_4 = \begin{bmatrix} 1 & 3 & 2 & 7 & 9 & 8 & 4 & 6 & 5 \end{bmatrix} \\
B_5 = \begin{bmatrix} 1 & 7 & 4 & 6 & 3 & 9 & 8 & 5 & 2 \end{bmatrix} \\
B_6 = \begin{bmatrix} 1 & 6 & 8 & 5 & 7 & 3 & 9 & 2 & 4 \end{bmatrix} \\
B_7 = \begin{bmatrix} 1 & 5 & 9 & 2 & 6 & 7 & 3 & 4 & 8 \end{bmatrix} \\
B_8 = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{bmatrix}
\]

Now equation (1) when applied to some BI, above, let say to BI2, it produces:

\[
C_{I1} = \begin{bmatrix} 1 & 7 & 4 & 2 & 8 & 5 & 3 & 9 & 6 \end{bmatrix} \\
C_{I2} = \begin{bmatrix} 1 & 6 & 8 & 5 & 7 & 3 & 9 & 2 & 4 \end{bmatrix} \\
C_{I3} = \begin{bmatrix} 1 & 4 & 7 & 3 & 6 & 9 & 2 & 5 & 8 \end{bmatrix} \\
C_{I4} = \begin{bmatrix} 1 & 8 & 6 & 9 & 4 & 2 & 5 & 3 & 7 \end{bmatrix}
\]

The following properties of AT are clear from the above experiments:

- Both of the transformation functions have different Arnold periodicities (4 in 1st case and 8 in 2nd).
- The scrambling patterns of both are different.
- Applying AT given in equation (1) to any of BI3s, we cannot retrieve back I.

In our proposed Steganography system model, we have exploited the above properties of the Arnold’s transformation to make the system more secure against unauthorized access.

4. PROPOSED MODEL

The proposed Steganography model has two phases: the embedding phase at the transmitter’s end and the extraction phase at the receiver’s end. In the embedding phase, the secret message S is first scrambled for some tm (assuming Pm is the period and 0 < tm < pm) number of times using Arnold’s cat map at a predefined m different levels [17], selecting m different transformation functions from equations (2) or equations (3), in a certain order O to make it more secure against unauthorized extraction. This scrambled message S’ is embedded into the cover image C to generate the stegoimage C’. C is transmitted and at the receiving end the secret message(s) is/ are extracted by following the extraction and decryption process in the reverse order. In this technique, the values of i, m, pm, tm, O are kept secret and are only known to the authorized users and extraction without the keys results with noises only, making the procedure secure.

4.1 Embedding Algorithm

INPUT: Cover image C of size N x N. Secret messages/images, let’s say; S1, S2, S3 of N x N blocks. Keys: i, m, pm, tm, O

For each message/image Sj, do step 1 to 3

STEP1: Scramble Sj with some Ai (where Ai is the i-th AT) for tm times to obtain Si

STEP2: Repeated step 1 for m number of times with different AT say Aj (j !=i) and tm's in order O to obtain final scrambled message Sj'.

STEP3: Embed the scrambled messages/images Sj's to the LSB planes of the cover image C to get the stegoimage C'.

4.2 Extraction Algorithm

INPUT: Stegoimage C’ of size N x N.
Keys: i, m, pm, p, tm, O

STEP1: Retrieve Si’s from the LSBs of C’.
For each Sj:
STEP2: Apply (pm - tm) times Arnold transforms Aj to obtain Si
STEP3: Repeat step 2 for m times with reverse order O to get back the secret messages Sj

5. EXPERIMENTAL RESULTS AND ANALYSIS

The proposed method is tested and validated over a range of 20 different standard gray scale images of size 128 x 128 including ‘Lena’ and ‘Baboon’ as the cover images. A number of binary images of size 128 x 128 including ‘Logo’, ‘Micky’ and ‘Text’ are considered as the secret messages/images for embedding purpose. Figure 4 (B, D) shows the stego images of original Lena and Baboon image after the secret messages are encrypted using the proposed method and embedded into the LSB, 7th and 6th bit planes of the cover images respectively.

Figure 5 shows the three least significant bit planes of the Lena image, which virtually contains no significant image information and seems like some random noises.

Figure 6 shows the information retrieved from the stego Lena image without using a valid key. It is clear from the figures that the information retrieved without a valid key is completely random, undetectable, unsuspicious and looks like some noise similar to that of figure 5. The secret information retrieved using the valid keys are given in figure 7.

For each message/image Sj, do step 1 to 3

STEP1: Scramble Sj with some Ai (where Ai is the i-th AT) for tm times to obtain Si

STEP2: Repeated step 1 for m number of times with different AT say Aj (j !=i) and tm's in order O to obtain final scrambled message Sj'

STEP3: Embed the scrambled messages/images Sj's to the LSB planes of the cover image C to get the stegoimage C'.

4.2 Extraction Algorithm

INPUT: Stegoimage C’ of size N x N.
Keys: i, m, pm, p, tm, O

STEP1: Retrieve Si’s from the LSBs of C’.
For each Sj:
STEP2: Apply (pm - tm) times Arnold transforms Aj to obtain Si
STEP3: Repeat step 2 for m times with reverse order O to get back the secret messages Sj
In case of single Arnold, as Arnold transform is periodic in nature, the information can be retrieved by running the algorithm for a certain number of times in random and observing the outputs. For example, figure 2.C, which is same as the original figure 2.A, can be retrieved from figure 2.B even without knowing the period p of the image and p’, the number of times Arnold transform is initially applied to it, just by systematically applying the transform somewhere between 1 to 3p number of times.

But in this proposed method the secret information remains highly secured and undetectable as the procedure involves a number of keys. It has been seen that it is not possible to reach at images of figure 7(A, B, C) by applying Arnold transform (AT) to images given in figure 6(A, B, C), a random number of times. Since the original message in this case is nothing but another scrambled image. So, the secret message remains highly secure against hit and trial extractions by unauthorized participants. The data hiding capacity of this method is also much higher in comparison the single LSB substitution method. Table I summarizes the comparison of this method against LSB substitution and simple Arnold Transform methods.

Table 1. Comparison of Image Steganography Methods

<table>
<thead>
<tr>
<th>Features</th>
<th>Single LSB substitution method</th>
<th>Simple Arnold Transform method</th>
<th>Proposed method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Imperceptibility</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>Capacity</td>
<td>Low</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>Robustness</td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>Encryption</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
</tr>
</tbody>
</table>

It has also been observed that the bit preservation ratio of the proposed method is better (most of the times) in comparison to the methods involving unscrambled data insertion.

This proves that the distortion to the original image is minimized against the unscrambled three bit substitution methods. The PSNR values [18] after embedding data into 1, 2, 3, 4 bit planes are given in Table II, which shows that the PSNR is as high as 37 dB even with 3-bit insertions.

Table 2. Text inserted into number of bit planes Vs PSNR

<table>
<thead>
<tr>
<th>Image (128 x 128) size</th>
<th>Embedding data in one Bit Plane</th>
<th>Embedding data in 2 Bit Planes</th>
<th>Embedding data in 3 Bit Planes</th>
<th>Embedding data in 4 Bit Planes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baboon</td>
<td>51.3797</td>
<td>43.6852</td>
<td>37.0031</td>
<td>30.8176</td>
</tr>
<tr>
<td>Lena</td>
<td>51.0937</td>
<td>43.4550</td>
<td>36.9229</td>
<td>30.4837</td>
</tr>
<tr>
<td>Miera</td>
<td>51.1843</td>
<td>43.4743</td>
<td>36.9133</td>
<td>30.5001</td>
</tr>
</tbody>
</table>

5. CONCLUSIONS

In spite of availability of a number of Steganography methods, research is still going on to develop methods satisfying all the requirements of Steganography. It is not that an easy task to develop a method that satisfies all the requirements as the requirements may vary with applications. Here we have implemented an algorithm that satisfies both of the attributes such as high imperceptibility & high security.
Being a spatial domain method, this of course, is not robust against noise, as the lower order bit planes are generally affected by noises and compression techniques. Future works in this direction include development of some transform domain methods those will provide robustness along with Impeccability, security and insertion into higher order bits to achieve further higher capacity and robustness.

6. REFERENCES


