Performance Analysis Of Secret Sharing Algorithm

Priya Metri, Department of Computer Engineering, MIT-COE, Pune, (M.H.) India
Sharmishtha Desai, Department of Computer Engineering, MIT-COE, Pune, (M.H.) India
Dr.S.T.Patil, Professor, Computer Engineering Department, VIT, Pune, (M.H.) India

Abstract
Handling secret has been an issue of prominence from the time for a human. Important things and messages have been always there to be preserved and protected from possible misuse or loss. If secret will be kept with group of people then reliability of the secret information increases. In this paper we proposed a secret image sharing algorithm based on Shamir’s secret sharing algorithm for gray scale and color images in different formats. Here we use (K,N) threshold sharing algorithm for secret image sharing along with image data hiding we use parity bit check policy for error detection to identify the tempering in image. Here, we divide the cover image into blocks of 2X2. We select each pixel value form a secret image and generate a pair of a share (x ,F(x)) using a Lagrange polynomial equation. We use (R,G,B) values of each pixel to hide the pixel values of secret image into cover image using LSB substitution method. For reconstruction original image we use polynomial interpolation formula for getting the original pixel values of secret image. We show the experimental result in terms of execution time for various types of secret images. In a proposed scheme execution time required for hiding process of a secret image is based on the size of image. We shown the comparative study of different techniques for secret image sharing based on various properties.

Keywords: Steganography, Secret Sharing, (K, N) Threshold, Least substitution Method, Pixel Value Differencing, DWT

Introduction
Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. For hiding secret information in images, there exists a large variety of steganography techniques some are more complex than others and all of them have respective strong and weak points. Steganography is the art of covered or hidden writing. The purpose of steganography is covert communication to hide a message from a third party. This differs from cryptography, the art of secret writing, which is intended to make a message unreadable by a third party but does not hide the existence of the secret communication. The steganography process generally involves placing a hidden message in some transport medium, called the carrier. The secret message is embedded in the carrier to form the steganography medium. The use of a steganography key may be employed for encryption of the hidden message and/or for randomization in the steganography scheme. In current techniques steganography can be categorized by the cover medium.

- Text Steganography
- Image Steganography
- Audio Steganography
- Video Steganography

This paper’s focus is on the review of steganography in digital images and a proposed scheme using Shamir’s secret sharing algorithm.

Literature Survey
Shamir proposed the first secret sharing scheme in 1979 designed to encode a secret data set into n shares and distribute them to n participants, where any k or more of the shares can be collected to recover the secret data, but any k -1 or fewer of them will gain no information about it. After the scheme was proposed, many related topics have been studied.

Chang-Chou Lin, Wen-Hsiang Tsai(2003) proposed a novel approach to secret image sharing based on a(K,N)-threshold scheme with the additional capabilities of steganography and authentication is proposed. A secret image is first processed into n shares which are then hidden in n user-selected camouflage images. It is suggested to select these camouflage images to contain well-known contents, like famous character images, well-known scene pictures, etc.

Pei-Yu Lin ,Chi-Shiang Chan proposed invertible image sharing approach in 2010. In this the revealed content of the secret image must be lossless and the distorted stego images must be able to be reverted to the original cover image. In order to achieve these purposes, they first transform the secret pixels into the m-ary notational system and then calculate the information data used to reconstruct original pixels from camouflaged pixels such that the information data and transformed secret data are shared using the (t,n)-threshold sharing scheme.

Ran-Zan Wang, Shyong-Jian Shyu (2007) proposed an innovative scheme, namely the scalable secret image sharing scheme, for sharing an image O among n partici-
pants such that the clarity of the reconstructed image (i.e., the amount of information therein) scales with proportion with the number of the participants.

Che-Wei Lee, Wen-Hsiang Tsai proposed (2010)[10] a new blind authentication method based on the secret sharing technique with a data repair capability for grayscale document images via the use of the Portable Network Graphics (PNG) image is proposed.

Related Work
I. Image Steganography
To hide information, straight message insertion may encode every bit of information in the image or selectively embed the message in “noisy” areas that draw less attention— those areas where there is a great deal of natural color variation. The message may also be scattered randomly throughout the image. A number of ways exist to hide information in digital media. Image steganography techniques are divided into two categories

a) Image steganography in spatial domain
b) Image steganography in frequency domain.

Steganography is broadly classified in to spatial and frequency domain technique. Least Significant Bit (LSB) replacement, LSB matching, Matrix embedding and Pixel value differencing are some of the spatial domain techniques.

Spatial domain steganographic techniques employ a simple technique in creating a covert channel in parts of the cover image which its method is to hide information in the least significant bit (LSB) of image data. Nevertheless, if lossy compression is used, the hidden information might be loss.

Another technique is the transform domain technique which it embeds information in the frequency domain of a signal and is much more robust than embedding principles that operate in the time domain. The advantage of this technique is it hides the information of image and less exposure to compression, cropping and image processing.

Spread spectrum technique is deal with the cover image as noise or try to add pseudo noise to the cover image. The cover image (noise) can add a single value to that cover image . As a result, the hidden data is spread through the cover image and unreadable to the third party.

II. Image Steganography Methods:
Least-Significant-Bits Substitution :
The most well-known steganographic technique in the data hiding field is least-significant-bits (LSBs) substitution proposed in [1]. The least significant bit i.e. the

eighth bit inside an image is changed to a bit of the secret message. When using a 24-bit image, one can store 3 bits in each pixel by changing a bit of each of the red, green and blue color components, since they are each represented by a byte. The embedding process consists of choosing a subset \( \{j_1, \ldots, j_\text{L(m)}\} \) of cover elements and performing the substitution operation LSB

\[
(c_{ji}) = m_i \quad (m_i \text{ can be either } 1 \text{ or } 0). 
\]

In the extraction process, the LSB of the selected cover-elements are extracted and used to reconstruct the secret message.

A Generic LSB-based Embedding Algorithm

Input :Cover C
For i=1 to Length(m) do
Compute index \( j_i \) where to store i
\( S_{j_i} \leftarrow \text{LSB}(C_{j_i}) = m_i \)
End for

Output:stego-object S

Advantages of LSB.
1. 100 % chances of insertion.
2. Easy to implement.
3. Not immune to noise and compression technique

Disadvantages of LSB.
1. One of the major disadvantage associated with LSB method is that intruder can change the least significant bit of all the image pixels. In this way hidden message will be destroyed by changing the image quality, a little bit, i.e. in the range of +1 or -1 at each pixel position.
2. Not immune to noise and compression technique

Steganography in the DCT Domain
One popular method of encoding secret information in the frequency domain is modulating the relative size of two (or more) DCT coefficients [7] within one image block. During the encoding process, the sender splits the cover- image in \( 8 \times 8 \) pixel blocks; each block encodes exactly one secret message bit. The embedding process starts with selecting a pseudo-random block \( b_i \) which will be used to code the ith message bit.

Let \( B_i = \text{D} \{ b_i \} \) be the DCT-transformed image block.

Before the communication starts, both sender and receiver have to agree on the location of two
DCT coefficients, which will be used in the embedding process;

**Algorithm**: DCT–Stegno encoding process

for \( i = 1, \ldots, (M) \) do

choose one cover-block \( b_i \)

\( B_i = D\{b_i\} \)

if \( m_i = 0 \) then

if \( B_i(u_1, v_1) > B_i(u_2, v_2) \) then

swap \( B_i(u_1, v_1) \) and \( B_i(u_2, v_2) \)

end if

else

if \( B_i(u_1, v_1) < B_i(u_2, v_2) \) then

swap \( B_i(u_1, v_1) \) and \( B_i(u_2, v_2) \)

end if

end if

adjust both values so that \( |B_i(u_1, v_1) - B_i(u_2, v_2)| > x \)

\( b_i = D^{-1}\{B_i\} \)

end for

create stego-image out of all \( b_i \)

**Algorithm**: DCT–Steg decoding process

for \( i = 1, \ldots, (M) \) do

get cover-block \( b_i \) associated with bit \( i \)

\( B_i = D\{b_i\} \)

if \( B_i(u_1, v_1) \leq B_i(u_2, v_2) \) then

\( m_i = 0 \)

else

\( m_i = 1 \)

end if

end for

**Statistical Steganography**

Statistical steganography techniques utilize the existence of “1-bit” steganographic schemes, which embed one bit of information in a digital carrier.

In order to construct a (m)-bit stego-system from multiple “1-bit” stego-systems, a cover is divided into (m) disjoint blocks \( B_1, \ldots, B_\text{(m)} \). A secret bit, \( m_i \), is inserted into the ith block by placing a “1” into \( B_i \) if \( m_i = 1 \). Otherwise, the block is not changed in the embedding process. The detection of a specific bit is done via a test function which distinguishes modified blocks from unmodified blocks. All the above mentioned algorithms for image steganography have different strong and weak points and it is important to ensure that one uses the most suitable algorithm for an application. All steganographic algorithms have to comply with a few basic requirements as shown in Table 1.

<table>
<thead>
<tr>
<th>Requirements</th>
<th>LSB</th>
<th>DCT</th>
<th>Statistical Techniques</th>
<th>(k,n) threshold secret sharing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invisibility</td>
<td>High*</td>
<td>High</td>
<td>Medium*</td>
<td>High</td>
</tr>
<tr>
<td>Robustness</td>
<td>Low</td>
<td>High</td>
<td>Low</td>
<td>Medium</td>
</tr>
<tr>
<td>Payload Capacity</td>
<td>High*</td>
<td>Low</td>
<td>Low</td>
<td>High</td>
</tr>
</tbody>
</table>

**Proposed Work**

In this paper we have proposed a technique using Shamir’s (K,N) threshold scheme for image steganography. Shamir's Secret Sharing is an algorithm in cryptography and is a form of secret sharing, where a secret is divided into parts, giving each participant its own unique part, where some of the parts or all of them are needed in order to reconstruct the secret. Counting on all participants to combine together the secret might be impractical, and therefore we sometimes use

\( f(B_i) = 1 \) block \( B_i \) was modified in the embedding process 0 otherwise the threshold scheme where any \( k \) of the parts are sufficient to reconstruct the original secret. Here we use \( n=3 \) images to hide a secret image in them and \( k=2 \) images which is a minimum number of shares we need to reconstruct the original secret image.

Algorithm for the construction of stegno image is as follows:

1. Secret image which we have to hide in Camouflage image.
2. Camouflage image to hide the secret image

**Algorithm**

**Step 1**: Accept both images.
**Step 2**: Generate integer array of pixel values for both images.
**Step 3**: Truncate (replace) pixel values in Camouflage image whose range is 251 to 255 with value 250.
**Step 4**: For each pixel in secret image and for each 2 X 2 block from camouflage image in sequential manner do
**Step 5**: Generate 2X2 image blocks of Camouflage image

**Step 6**: Take the value \( x_i \) of the top-leftmost pixel \( X_i \) of each camouflage image block \( B_i \) as the value \( x \).
**Step 7**: Take the value \( s \) of the secret image pixel \( S \) as the value \( y \).
**Step 8**: Choose arbitrarily a set of \( k \)-1 integer values for use as the \( m_i \). Here we take \( k=2 \).
**Step 9**: For each \( x_i \), compute the corresponding value of \( F(X_i) \) using equation

\( F(x) = \lceil y + m_1 \times x + m_2 \times x^2 \ldots..m_{k-1} \times x^{k-1} \rceil \)
Here value of $q$ is 251. As $k=2$ our equation will of a 
form and we have to take two values of $m$ ie $m_1, m_2$. 
$F(x)=[y+m_1 * x + m_2 * x^2] \mod q$

**Step 10**: Convert value of $F(x)$ to 8 bit. Hide the eight 
data bits of $F(x)$ in the data bits of the three pixels $W_i$, 
$U_i$, and $V_i$ of the corresponding camouflage image block 
$B_i$ Generate the Stegno image and display the resulting 
image.

**Process For Secret Image Recovery With Stego- 
Image Authentication.**

**Steps:**

**Step 1**: Divide each stego-image into block each of the 
size of 2 X 2.

**Step 2**: For each stego-image perform the following 
steps to recover the secret image pixel $S_i$.

**Step 3**: For each image block take the value $x_{ji}$ of 
the top-leftmost pixel $X_{ji}$ of the 2 X 2 stego-image block 
$B_{0ji}$ as a value of $x_j$ appearing in Eq in algorithm 1 extract 
the data bits of $F(x)$ from those of the three pixels 
$W_{ji}$, $U_{ji}$, and $V_{ji}$ of $B_0$.

**Step 4**: Compute, by the use of equation given below the 
corresponding value of $y$ as the value $s_i$ for the secret 
image pixel $S_i$ in terms of the values of all $x_j$ and $F(x)$.
Compute the reconstruction coefficients $F(x)$ according 
to equation

$$F(x)\equiv \prod_{i=1}^{n} (x - x_i)$$

Compute $f(0) = F(0) = \prod_{i=1}^{n} (-x_i)$

**Step 5**: Compose all the secret image pixels to form the 
desired $m \times m$ secret image $S$ as output and stop the 
algorithm.

**Experimental Work**

To evaluate the performance of the proposed 
scheme, several experiments were conducted by using 
Java Platform in Windows 7 environment. We compared 
the experimental results for the proposed algorithm in 
terms of execution time for different gray scale and color 
images in various formats as shown in Table 2.

**Conclusion**

In this paper we had proposed a secret image sharing 
technique whose result shows that processing time for 
the proposed algorithm is based on type and size of 
secret image. We have shown that in a proposed scheme 
execution time required for hiding process of a secret 
image is based on the size of image. The algorithm is 
implemented in JAVA using Net beans. We used 
JFrames for displaying the resulting images. We used a 
AWT packages for image processing purpose and meth-
od associated with it.

Also we reviewed different methods of steganography. 
As it is shown, each method has a procedure of embed-
ding for itself, and each one have some advantages, and 
also disadvantages in comparison with other methods of 
steaganography. So it is not possible to say that a speci-
ified method is the best method and best off all. Either, 
it’s impossible to determine the worst one. We can just 
compare them from different aspects, which results in 
determining a suitable method for a specific usage. We 
have also explained the way each algorithm works. It can 
help the reader proportionally to understand why an al-
gorithm is better than another in a specific situation.

**Reference**

in images by simple LSB substitution”, Depart-
ment of Computer Engineering and Information 
Technology, City University of Hong Kong, Hong 
Kong Received 17 May 2002; received in revised 
form 11 July 2003; accepted 11 August 2003.

data in images by optimal moderately significant-bit 
1017–1018.

for images by pixel-value differencing.Pattern R e-
cogn Lett 24:1613–162


[10] Che-Wei Lee, Student Member, IEEE, and Wen-Hsiang Tsai, Senior Member, IEEE“A Secret-Sharing-Based Method for Authentication of Grayscale Document Images via the Use of the PNG Image With a Data Repair Capability” IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 21, NO. 1, JANUARY 2012