Adaptive Data Hiding Based on Visual Cryptography

M. Padmaa and Y. Venkataramani
Saranathan College of Engineering, Trichirapalli, Tamil Nadu, India

Abstract: Signals, images, emails, voice and videos, everything comes under screening before or after it is communicated. Protecting the information is highly essential especially in electronic communication which has become a stipulation in the routine life of zillions. Since safeguarding has many literal connotations, this study narrates on one of them, privacy; technically secrecy or security. From the family of Information security, the proposed method can pick out cryptography and steganography to make this algorithm more secure and effective as well. As far as Visual Cryptography is concerned, the primary terminologies here are share, user and transparency. Its blend with steganography is worth mentioning here as it forms a new platform in information security and secret sharing. For embedding, Pixel Indicator (PI), Pixel Value Differenting (PVD) and OPAP are used. With reference to Pixel Indicator, two methods are discussed here. The effectiveness of the proposed method is assessed by calculating MSE and PSNR and the outcomes are tabulated and compared with existing methods.

Key words: Visual cryptography, pixel indicator, pixel value differencing, steganography

INTRODUCTION

At the budding of security developments, cryptography was introduced which completely destroys the user perspective of viewing and transforms the content to something that is unrecognized data. This could sustain for basic security, but as the threats started rising, cryptography succumbed as the process is well known to the viewer. As an enhancement, method whose changes are unperceivable irrespective of any operation was required. This got steganography and watermarking to limelight (Stefan and Fabin, 2000). Cryptography is an art of providing data security using methods of encryption and decryption (Schneier, 2007).

Cryptography lends a helping hand in keeping information safe and sound (Schneier, 2007). This is its ultimate aim for which the modern era version has come up with vast and different practices and procedures for real time application. Scores of cryptic algorithms are formulated for security’s sake and of which the one that has recently found surprising is the expense of Visual Cryptography (Noar and Shamir, 1995; Amirtharajan et al., 2013a, b). It of course, has its origin from conventional cryptography. In simple words to put it, message to be communicated (secret) to the other end undergoes segmentation and is sent in operated forms. Thus, at the receiving end, one has to merge all the segments in a right way to read the secret.

Visual cryptography is a branch of cryptography concerned with providing data security using black and white pixels. As the name indicates, visual cryptography is based on human vision. It uses the characteristics of human vision to decipher the original message from the scrambled or encrypted images. It is an emerging trend of cryptography which uses the concept of shares. It assumes that the message consists of black and white pixels and each pixel appears in ‘n’ modified forms. These modified forms are called shares (Noar and Shamir, 1995; Amirtharajan et al., 2013a, b). Unlike other techniques, it does not require any knowledge of cryptography techniques. Also, it does not require any complex computations. Hence it is simple and self-sufficient in providing data security. Visual cryptography guarantees that hackers cannot comprehend the ideas about a secret image from different cover images. For instance, if there are ‘n’ images, then there shall be a constant ‘k’ of such images. Hence the secret can be revealed with ‘n’ or ‘n-1’ such images but not just with ‘k’ images. This comes from the fact that the output media of visual cryptography are transparent as shown in Fig. 1. This term evolves from the way the white pixels of black and white images are considered as transparent. This method, also known as the black and white visual cryptography breaks down every pixel of the secret image into a 2^3 block. Hence the cover can be shared among a group of ‘n’ people.

Steganography invented by the Greek is a method of “covered writing” where only the beneficiary knows the existence of the secret message apart from the sender, even if were available on a public forum (Amirtharajan et al., 2011, 2012, 2013c-i,
MATERIALS AND METHODS

Cryptography enables information security by employing techniques in which the data is scrambled by a key in the process called encryption and re-scrambling the encrypted message again with the key in order to get back the original data in the process called decryption. Here, the key plays a vital role. Without the correct key, the scrambled message cannot be recovered (Hou, 2003). Visual cryptography assumes that the message consists of black and white pixels and each original pixel appears in n modified versions called shares (Amirtharajan et al., 2013a-b). Each share is a collection of m black and white sub pixels and is generated by doing mathematical operation between subset (n x m) of original message and permuted version of any one of the two (n x m) random matrix Noar and Shamir (1995).

In Steganography the confidential information is embedded into innocent looking cover objects, such as digital images (Chang et al., 2003; Chang and Tseng, 2004; Chan and Cheng, 2004; Cheddad et al., 2010; Thainkaiselvan et al., 2011a-b, 2013). In this proposed method, visual cryptography and tri color random image steganography is combined for multiple users. Figure 2 represents the basic block diagram for this proposed method. For embedding, input color image can be taken as secret. To make encryption easy, color image should be converted into gray scale image. Dithering is used to convert gray image into binary image. By using (k, r) threshold scheme, shares are generated (Noar and Shamir, 1995) and these shares are once again encrypted with different keys. Then these encrypted shares are embedded in the cover image using Pixel indicator method.

In pixel indicator method (Gutub, 2010; Padmaa et al., 2011; Padmaa and Venkataratamani, 2010) any one of the color plane is treated as indicator plane and remaining two planes are used to embed the data. The color plane for data embedding is decided by the last two bits of the pixel of indicator plane. The number of bits to be embedded is decided by calculating the difference value d between the maximum pixel value and the minimum pixel value of three neighbor pixels (Padmaa et al., 2011) and the quality of stego image is enhanced by OPAF method (Chan and Cheng, 2004). There are more explanation on steganography methods and its advantages are available in Amirtharajan et al. (2011, 2012, 2013a-i) and Zanganeh and Ibrahim (2011). For recovery, stego image is considered. Based on the last two LSB bits of each pixel in the indicator plane, the shares are recovered by using PVD method and then descrambled by using the keys (Gutub, 2010). These descrambled shares are stacked and
EMBEDDING ALGORITHM

**Method 1:**
- Read the Cover image (U) and Secret image (S)
- Apply (k, n) Threshold scheme to secret image which constructs four shares of this secret image say S1, S2, S3 and S4
- Divide the color cover image into three planes (Red, Blue and Green)
- In this first method, take the default indicator as Red and perform the following
  - Let r[0] = First LSB of current pixel in Red plane
  - Let r[1] = Second LSB of current pixel in Red plane
  - If r = 00, then
    - No entranching, move to next pixel
  Else if r = 01, then
    - Scramble the first share of secret image S1 with key K[1], then embed the scrambled first share S1 in current pixel of Red plane by means of PVD
  Else if r = 10, then
    - Scramble the second share of secret image S2 with key K[2], then embed the scrambled second share S2 in current pixel of Blue plane by means of PVD
  Else
    - Scramble the third and fourth shares of secret image S3 and S4 with key K[2], then embed the scrambled shares in both the planes by means of PVD
- Once all the shares are embedded, apply OPAP to get the Stego image (V)

**RECOVERY ALGORITHM**

- Read the Stego image (V) and split into three planes
- To retrieve the embedded shares of secret image, verify the last two bits of the Indicator plane
  - If r = 00, travel to next pixel
  - Else if r = 01, then
    - Recover the First share S1 from Green plane by means of PVD and descrambel it with key K[1]
  - Else if r = 10, then
    - Recover the second share S2 from Blue plane by means of PVD and descrambel it with key K[2]
  - Else
    - Recover the third and fourth share S3 and S4 from Green and Blue planes by means of PVD and de-scramble it with keys K[3] and K[4], respectively
- If all the shares are recovered, combine it to acquire the Secret image (S)

**Method 2: Embedding algorithm**
- Read the Cover image (U) and Secret image (S)
- Apply (k, n) Threshold scheme to secret image which constructs four shares of this secret image say S1, S2, S3 and S4
- Divide the color cover image into three planes (Red, Blue and Green)
- In this method, Indicator planes are chosen in a cyclic manner
  - Let r[0] = Indicator plane, r[1] and r[2] = Data Channel 1 and 2
  - Let r[0] = First LSB of current pixel in Red plane
  - Let r[2] = Second LSB of current pixel in Red plane
- If r = 00, then
  - No entranching, move to next pixel
  Else if r = 01, then

Fig. 2: Block diagram of proposed method
RESULTS AND DISCUSSION

In this execution, four cover color images Lena, Baboon, Mahatma Gandhi and Temple of size 256×256 are chosen for embedding. The cover and stego images along with their histograms are shown in Fig. 3-10. This algorithm is simulated in MATLAB 7.1. To have an idea about effectiveness of the system, MSE, PSNR, BPP and embedding capacity are calculated and tabulated in Table 1, 2 and 3. The equations are:

\[
\text{MSE} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} (C_{ij} - S_{ij})^2
\]

\[
\text{PSNR} = 10 \log_{10} \left( \frac{I_{max}^2}{\text{MSE}} \right) \text{dB}
\]

Embedding Capacity = Bits per pixel×No. of pixels in the cover image

For the chosen images, full embedding capacity for the two methods is examined here. Method 1 takes RED as indicator, as per the algorithm no embedding is done in this plane. It is clear from the table that all the images

<table>
<thead>
<tr>
<th>Table 1: MSE, PSNR values for method 1</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cover image</strong></td>
</tr>
<tr>
<td>------------------</td>
</tr>
<tr>
<td>Lena</td>
</tr>
<tr>
<td>Baboon</td>
</tr>
<tr>
<td>Mahatma Gandhi</td>
</tr>
<tr>
<td>Temple</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 2: MSE, PSNR values for method 2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cover image</strong></td>
</tr>
<tr>
<td>------------------</td>
</tr>
<tr>
<td>Lena</td>
</tr>
<tr>
<td>Baboon</td>
</tr>
<tr>
<td>Mahatma Gandhi</td>
</tr>
<tr>
<td>Temple</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 3: Comparative estimation parameters of the proposed embedding method 2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cover image</strong></td>
</tr>
<tr>
<td>------------------</td>
</tr>
<tr>
<td>Lena</td>
</tr>
<tr>
<td>Baboon</td>
</tr>
<tr>
<td>Mahatma Gandhi</td>
</tr>
<tr>
<td>Temple</td>
</tr>
</tbody>
</table>

For the chosen images, full embedding capacity for the two methods is examined here. Method 1 takes RED as indicator, as per the algorithm no embedding is done in this plane. It is clear from the table that all the images
Fig. 3(a-b): (a) Cover and (b) Stego images of Lena and their corresponding histograms.
Fig. 4(a-b): (a) Cover and (b) Stego images of Baboon and their corresponding histograms.
Fig. 5(a-b): (a) Cover and (b) Stego images of Mahatma Gandhi and their corresponding histograms
Fig. 6(a-b): (a) Cover and (b) Stego images of Temple and their corresponding histograms
Fig. 7(a-b): (a) Cover and (b) Stego images of Lena and their corresponding histograms
Fig. 8(a-b): (a) Cover and (b) Stego images of Baboon and their corresponding histograms.
Fig. 9(a-b): (a) Cover and (b) Stego images of Mahatma Gandhi and their corresponding histograms
Fig. 10(a-b): (a) Cover and (b) Stego images of Temple and their corresponding histograms.
exhibit high PSNR. In general, PSNR of above 38 dB is rendered good. So, all these images possess high PSNR, which indicates high imperceptibility; that is the images are prone to visual attack and escape it. Thus one cannot sense the hidden data in the images. Conversely, MSE is very low. But Baboon has relatively high MSE of all. In turn it has the highest embedding capacity. Relatively decent BPP is obtained in all images. Also, high embedding capacity highlights this routine. Indicator is cyclically selected in method 2, where each plane will have a chance of being the indicator. The images possess high BPP and also embedding capacity is also high. Approximately, 2.64/5 bits are embedded in each plane which is determined to be fair. Thus, method 2 gives anticipated results and is best. This method exhibit higher imperceptibility, security and is highly robust to steganalytic attacks.

Comparison of existing methods with proposed method:
In pixel indicator method (Padmaa et al., 2011), any one of the colour planes is assumed to be the indicator and data is embedded accordingly. In pixel authorised by pixel with pixel indicator method (Amirtharajan and Rayappan, 2012c), Hilbert SFC and Moore SFC traversing path based steganography techniques are applied. Here a block of 4x4 pixels are taken and the above methods are implemented on it by adapting a common traversing path for the sender and receiver. Then the entire cover image is taken for secret bit embedding by considering it as multiple 4x4 blocks to cover up the entire 2x2x3 pixels. The pixel indicator method here is used to select a particular channel as an indicator. Then data embedding in other channels is done based upon the last two bits of the indicator.

CONCLUSION

In this proposed method, Cryptography, Visual Cryptography and Steganography are put together to enhance the security and robustness. The method minimizes the perceptibility of the introduced distortion. Compared with Pixel indicator and Pixel authorized by pixel to trace with Pixel indicator methods, our proposed method makes stego-image so strong. Four parameters namely MSE, PSNR, BPP and embedding capacity are used as metrics for comparison. Visual cryptography with steganography will provide minimum MSE and maximum PSNR and moderate embedding capacity. These parameters decide the imperceptibility and robustness of a stego-image. This method provides better resistance against various forms of attacks.

ACKNOWLEDGMENT

The first author expresses her sincere gratitude to Dr. R. Amirtharajan Associate Professor/ECE School of Electrical and Electronics Engineering, for his guidance in providing technical and linguistic support for fructifying the quality of this study.

REFERENCES


