ENHANCED IMAGE SECRET SHARING THROUGH VIDEO USING TWO DECODING OPTION

1Sai Vignesh, 2K.B.Gurumoorthy, 3N.Deepak

1Student Btech, 2Assistant professor, 3Assistant professor
E-mail: sa1.1002121@srec.ac.in, gurukb85@gmail.com, Deepak.n@srec.ac.in

Abstract- Visual Cryptography Scheme is one of the recent emerging areas in image secret sharing, where one can easily encrypt and share the image in secure way and which can be decrypted through the human visual system without computation. In this project, this scheme is implemented for hiding image in a video stream using two in one image secret sharing scheme (TiOISSS) with two decoding options. It is based on Visual Cryptography Scheme (VCS) and Polynomial based image secret sharing scheme (PISSS) known as Newton’s raphson method and comparing the same with already existing Lagrange’s interpolation method. This comparison is made to show the reduction in file size of shadow image for faster transmission within a distributed multimedia system.

Keywords- secret sharing, Visual Cryptography Scheme (VCS), Polynomial-based Image Secret Sharing Scheme (PISSS) – Lagrange’s Interpolation and Newton-Raphson’s method.

I. INTRODUCTION:

Now -a- days it is very common to share the multimedia data via internet, there is an urgent need to secure the information in open network environment. The image secret sharing scheme is one of the commonly used schemes to share the secret image. This ISSS is classified into two categories – Visual cryptography scheme and polynomial based secret sharing scheme. An image secret sharing scheme (ISSS) divides a secret image into some shadow images (known as the shadows) in a way that requires the shadows in a certain privileged coalitions for the secret reconstruction. However, the secret image cannot be revealed if they are not combined in the prescribed way. ISSS is often referred to as a (k, n)-threshold scheme, where k is the threshold value to reveal the secret and n denotes the number of shadows used. A secret image is reconstructed by using k or more than k shadows, but it cannot be done with the shadows less than k.

In this (k, n) – VCS, where k ≤ n, a secret image is encrypted into n shadows by expanding each secret pixel into m (referred to as the pixel expansion) subpixel. The difference between the pixel and the subpixel is that the “pixel” denotes the secret pixel located in the secret image, and the “subpixel” means the pixel present in shadows. The size of a sub pixel and the secret pixel is same. As said above, anyone can photocopy their shadows on transparencies and stack them to decode the secret visually through the human visual system (HVS). But no information is gained with (k-1) shadows. The first VCS encrypted a halftone (black-and-white) secret image into noise-like shadows; subsequently, most VCSs were dedicated to reducing the pixel expansion. Some of them even had a non-expandable shadow size. Other VCSs for sharing the gray and chromatic secret images were proposed to achieve more applications.

Noise-like shadows of VCS, however, were suspect to censors and difficult for identification and management. Most people are indeed not fond of the poor visual quality of VCS, which comes from its intrinsic property using the OR-operation for decoding. As is known, the monotone property of the OR-operation causes such visual effects that a black subpixel in one of the transparencies cannot be undone by the color of another subpixel in other transparencies laid over it. On the contrary, PISSS can recover the secret image without any distortion, while it needs the computation. By directly adopting Shamir’s secret sharing scheme, a (k, n)-PISSS takes the secret pixel as the constant term in the (k−1)-degree polynomial to share the secret. Thien and Lin used all coefficients of the polynomial to reduce shadow with size 1/k times that of the secret image. Afterwards, the shadow size is further reduced by using the Huffman code. Both PISSSs had noise-like shadows. The user-friendly (k, n)-PISSS produced the shadow representing a shrunken secret. PISSS with the authentication capability in a recently emerging research, where the authors added the authentication by embedding the shared bits and authentication bit (total of nine bits) in a 4-pixel block.

A new type of ISSS with two decoding options was introduced recently, where the secret image is revealed both by stacking the transparencies and by computation. This scheme is referred to as the two-in-one ISSS (TiOISSS). This utility TiOISSS can decode secret images for preview by HVS when a computer is temporarily unavailable. When the computer is available during the decoding scene, we then spend more computation to obtain a high-quality image for high-end applications. So far, two TiOISSSs have been proposed. Both schemes can stack shadows to decode a halftone secret image by HVS in the first stage, and they can perfectly reconstruct the gray-level secret image in the second
stage. A possible application scenario of TiOISSS is described below. In a distributed multimedia system, the n shadows of PISSS can be delivered in a distributed system where each shadow is stored in any distributed storage node. In this application, the failure of (n-k) shadows during transmission does not affect the reconstruction phase, as the secret image can be perfectly restored using k shadows. Suppose a fake shadow is received.

The receiver may spend considerable computation and finally find the received shadow is wrong. Because the reconstruction phase of PISSS is very computationally intensive, we can therefore apply the TiOISSS to save the computational time for verifying of the validity of shadows. The receiver can first verify the shadows by visually previewing the secret without computation. After the successful verification, the receiver then recovers the original gray level secret image by computation.

In this paper, we design a new TiOISSS by properly combining VCS and PISSS to develop their specialities and simultaneously avoid the disadvantages. When compared with the previous TiOISSSs (Lagrange’s interpolation method), our scheme (Newton’s Raphson method) has the lesser shadow size. The rest of this paper is organized as follows: Section 2 reviews PISSS and VCS. The proposed framework is introduced in Section 3, and experimental results and comparisons are given in Section 4 and Section 5 concludes the paper finally.

II. PRELIMINARIES:

The design implemented is based on TiOISSS where PISSS and VCS are combined used for perfect reconstruction and less time consumption.

2.1. Polynomial-based Image Secret Sharing (PISSS):

A polynomial-based (k, n) secret sharing scheme was firstly proposed by Shamir, in which the secret data is encrypted into n shadows.

Any k shadows can be used to reconstruct the secret, but any k–1 or fewer shadows get no information.

2.1.1. Lagrange interpolation method:

The simplest form of interpolation is to approximate two data points by a straight line. By taking the secret data as f0 (constant term) in the following (k–1)-degree polynomial f(x), where p is a prime number, we could construct n shadows

\[ f(x) = f_0 + f_1 x + \ldots + f_{k-1} x_{k-1} \mod p. \]  

(1)

Where \( f_0 \) - Secret data

\( p \) - Maximum prime number

By using this Lagrange interpolation method, the shadow size is reduced by 1/k times of the secret image by embedding the secret data in all the coefficients of f(x).

2.1.2 Newton Raphson’s method:

The Newton Raphson method is a powerful technique for solving equation numerically. Like so much of differential calculus it is based on simple idea of linear approximation. This method is mainly used for effective results and to reduce the file size.

If \( x_i \) is the initial guess at the root, a tangent can be extended from the point \([x_i, f(x_i)]\). The point where this tangent crosses the x-axis usually represents an improved estimate of the root. The Newton Raphson can be derived on the basis of this geometrical interpretation. The first derivative \( f'(x) \) is equivalent to the slope.

\[
\frac{f'(x_i)}{f''(x_i)} = \frac{f(x_i) - 0}{x_i - x_i + 1}
\]

(3)

This can be rearranged to yield

\[ x_{i+1} = x_i - \frac{f(x_i)}{f'(x_i)} \]

(4)

Thus, the main advantage of using Newton Raphson method is faster convergence of the root and it is easy to convert to multi-dimensional image.

2.2. Visual Cryptography Scheme (VCS):

Since Naor and Shamir proposed the basic model of visual cryptography. Many related studies have been published by researchers. The first VCS were Naor-Shamir’s (k, n)-VCS to encrypt a halftone secret image into noise-like shadows. In which they used the whiteness (the number of white sub pixels in a m-sub pixel block) to distinguish the black color from the white color, i.e., “m−‘h’B’h’W (respectively “m−l’B’T’W) represents a white (respectively black) color, where hNI. A black-and-white (k, n)-VCS can be designed using two base n×m matrices B1 and B0 with elements “1” and “0” denoting black and white sub pixels.

When sharing a black and white secret pixel, one row of the matrix in the set C1 and C0 is chosen respectively includes all matrices obtained by permuting the columns in B1 and B0 respectively to a relative shadow. Let OR (B1r), i=0, 1, denote the “OR”-ed vector of any r rows in Bi, and H (·) be the Hamming weight of a vector. Then, the base matrices of the (k, n)-VCS satisfy the following conditions:

1. \( (V-1), H(OR(B_1r)) \geq (m-l) \text{ and } H(OR(B_0r)) \leq (m-h) \)

(5)

For \( k \), where \( 0 \leq l < h \leq m. \)
2. \((V-2).H(\text{OR}(B_{i1}|r))= H(\text{OR}(B_{i0}|r))\)
For \(r \leq (k-1)\).

(6)

The first condition is often referred to as the contrast condition, and the secret image can be recognized due to their different contrasts of black and white colours. The second condition is the security condition that assures the \((k, n)\)-VCS of perfect secrecy.

III. PROPOSED FRAMEWORK:

As is known, PISSS has a perfect reconstruction and spends the competition for reconstruction it is reasonable to adopt in a Two in One Scheme where the secret image and host image can be revealed both by stacking the transparencies and by competition. In PISSS method of Lagrange interpolation, for a given points \(x_j\) and \(y_j\), the Lagrange polynomial is the polynomial of least degree that at each point \(x_j\) assumes the corresponding value \(y_j\). The fact that changing the interpolation points requires recalculating the entire interpolant we make use of Newton polynomials which is easier to use. Newton’s method(also known as the Newton-Raphson method), named in such a way after Isaac Newton and Joseph Raphson, is used to find successively better approximations to the roots(0r zeros) of a real valued function.

The compression version which is proposed by Lin et al.’s compresses the secret image such that the shadow size has enough space to hide the information of a compressed image. Obviously, this approach can be extended to the lossless version by expanding the half tone image with a size \(|F'| = \left(\frac{2}{k}\right)^2 |I| \times 8/\log2(m)\) to hide the original host image. For the lossless version of Lin et al.’s TIOSSS, the pixel expansion \(m_{LIN}\) is

\[m_{LIN} = \left(\frac{2}{k}\right)^2 m \times 8/\log2\left(\frac{m}{w}\right),\]

where \(I'\) is the gray scale image, \(m\) is the pixel value, \(w\) is the white pixel value, \(n\) is the number of shadows, \(k\) is the threshold value.

Algorithm 1: (encryption algorithm)

Input: The gray level secret image \(I\), Parameter: \(k, n, m, f\)
Output: \(n\) shadow \(F_i\)
  I. Encrypt the secret image to obtain \(P_i, P(I), i \in [1, n]\).
  II. Obtain \(I'\) from \(I' = H(I)\).
  III. Output \(n\) shadows \(F_i = F(I'), i \in [1, n]\).

Algorithm 2: (decryption algorithm)

Input: any \(k\) out of \(n\) shadows \(F_{i1}, F_{i2}, \ldots, F_{ik}\)
Output: the halftone secret image \(I'\) and gray-level secret image \(I\)

/* Phase 1: does not need computation; visually decode the secret \(I'\) by stacking \(k\) shadow;
Phase 2: needs computation; decode the secret \(I\) by using Lagrange interpolation and newton’s raphson method. Perfect reconstruction is obtain from this phase*/

IV. EXPERIMENTAL RESULTS AND ANALYSIS:

Here some experimental results are analysed to prove the feasibility of the proposed scheme. In the above experiments,
1. First extract a frame from the video, refer fig (a).
2. Then take an image shown in fig (b) as the secret image.
3. After applying the Newton Raphson method to the image we get shadow image as shown in fig(c) and fig (d).
4. In the phase of recovery, we perform 'bit or’ operation to decrypt the secret image, refer fig (e).
5. We are working on the process of inserting the encrypted image in a video and in the receiver side the frame is extracted again and the secret image is retrieved.
4.1. Comparison:
In the Lagrange interpolation method, polynomial can be written down without the solution of linear system of equation. In this basis polynomial depend only on \( x_1, x_n \) not on values of \( p \). The chief reason, for the extensive use of Newton-Raphson is its accuracy and efficiency. The reason for its accuracy is number of significant digits in the solution doubles at every iteration. The pixel expansion and the file size of the shadow image are compared for Lagrange and Newton’s method in Table 1 and represented graphically in Fig – f.

Table 1: Pixel expansion and file size of image

<table>
<thead>
<tr>
<th>((k, n))</th>
<th>(B_1)</th>
<th>(B_0)</th>
<th>Lin et al.’s TIOSSSSS</th>
<th>Lagrange Interpolation</th>
<th>Newton Raphson’s method</th>
</tr>
</thead>
</table>
| \((2, 2)\) | \[
    \begin{bmatrix}
    1 & 0 \\
    0 & 1 \\
    \end{bmatrix}
    \] | \[
    \begin{bmatrix}
    1 & 0 \\
    1 & 0 \\
    \end{bmatrix}
    \] | 16 | 33,554,432 | 1 | 2,097,152 | 2/3 | 1,854,236 |
| \((2, 2)\) | \[
    \begin{bmatrix}
    1 & 0 & 0 \\
    1 & 0 & 1 \\
    \end{bmatrix}
    \] | \[
    \begin{bmatrix}
    1 & 1 & 0 \\
    1 & 0 & 0 \\
    \end{bmatrix}
    \] | 15.14 | 31,750,880 | 3/4 | 1,572,864 | 2/5 | 1,258,421 |
| \((2, 3)\) | \[
    \begin{bmatrix}
    1 & 0 & 0 \\
    0 & 1 & 0 \\
    \end{bmatrix}
    \] | \[
    \begin{bmatrix}
    1 & 0 & 0 \\
    1 & 0 & 0 \\
    \end{bmatrix}
    \] | 22.71 | 47,626,320 | 3/2 | 3,145,728 | 1 | 2,836,427 |
| \((2, 3)\) | \[
    \begin{bmatrix}
    1 & 0 & 0 \\
    0 & 1 & 1 \\
    \end{bmatrix}
    \] | \[
    \begin{bmatrix}
    1 & 1 & 0 \\
    1 & 0 & 1 \\
    \end{bmatrix}
    \] | 22.71 | 47,626,320 | 3/4 | 1,572,864 | 2/5 | 1,258,421 |
CONCLUSION:

The scheme used here is a hybrid of Polynomial Image Secret Sharing and Visual Cryptography. In this paper, comparison is made between Lagrange and Newton Raphson’s method for the further enhancement of secret data. By using these threshold schemes the secret image will be decoded perfectly along with the reduction in file size and also for the faster transmission in the multimedia system. Thus the Newton Raphson’s method is better than Lagrange’s Interpolation for the further reduction in file size of secret data.

REFERENCES: