Verifiable Image Secret Sharing Using Matrix Projection

N F Azzahra* and K A Sugeng*

1Department of Mathematics, Faculty of Mathematics and Natural Sciences, Universitas Indonesia, Indonesia
*Corresponding Author. nurfathiyafrdn@gmail.com; kiki@sci.ui.ac.id

Abstract. Secret sharing scheme is a technique to share secret data into \( n \) pieces based on a simple \((k, n)\) threshold scheme. However, the problem with Shamir’s secret sharing scheme is that they do not provide any way to verify that the dealer was honest and the shares were indeed valid. This problem also occur in the Thien and Lin’s image secret sharing or the Li Bai’s construction using matrix projection. On the other hand, a developed protocol for secret sharing called verifiable secret sharing allows every participant to validate their received piece to confirm the authenticity of the secret. Therefore, this paper discussed a proposed scheme based on verifiable secret sharing, in which the matrix projection is used to create image shares and a public matrix from watermark image. The secrets were represented in elements of a square matrix. The watermark image was used for verifiability where the reconstructed watermark image verifies the accuracy of the reconstructed secret image.

1. Introduction
Secret sharing scheme is a technique to share secret data into \( n \) pieces based on a simple \((k, n)\) threshold scheme, in which participants will easily reconstruct the secret if there are minimum \( k \) pieces while knowledge of any \( k - 1 \) pieces will not be able to decipher the secret [5]. An extension to Shamir’s secret sharing scheme on images proposed by Thien and Lin image secret sharing [6]. In which, the generated image shares or shadow images are smaller than the secret image. Another extension of Shamir’s scheme also applied in Li Bai’s method of generating an image shares using matrix projection [1, 2]. However, there is no guarantee in both schemes that they prevent dishonest dealer or shareholders.

On the other hand, a developed protocol for secret sharing called verifiable secret sharing allows every participant to validate their received piece to confirm the authenticity of the secret. Wang et al. developed a method for sharing a secret image with verification, in which an \( m \times m \) watermark image is used to verify the accuracy of the reconstructed image [7].

2. Secret Sharing Scheme
Secret Sharing Scheme is a technique to secure secret data in which the data will be divided into shares, with each participant received one share, and the secret data will only be revealed if put together according to the predefined combinations [5].

2.1. Shamir’s Secret Sharing Scheme [5]
Shamir developed a scheme to divide data \( D \) into \( n \) shares \( D_1, D_2, \ldots, D_n \) such that it takes \( k \) pieces or more of \( D_i \) to determine \( D \), and the knowledge of \( k - 1 \) pieces of \( D_i \) will not be able to decipher the secret. This is called \((k, n)\) threshold scheme. Shamir’s secret sharing scheme is using the idea of
polynomial interpolation in which given \( k \) different points with \( i = 1, 2, \ldots, k \), there is only one polynomial \( q(x) \) of degree \( k - 1 \) such that \( q(x_i) = y_i \) for each value of \( i \). When \( D \) is assumed to be a number, then to divide \( D \) into \( D_i \), choose \( q(x) = a_0 + a_1 x + \cdots + a_{k-1} x^{k-1} \) where \( D = a_0, \) and \( D_1 = q(1), \ldots, D_i = q(i), \ldots, D_n = q(n) \). The knowledge of \( k \) pieces of \( D_i \) will determine the coefficient of polynomial \( q(x) \), and the value of \( D = q(0) \) will be able to be calculated. On the other hand, knowledge of \( k - 1 \) pieces of \( D_i \) will not be enough to calculate the value of \( D \).

2.2. Thien and Lin’s Image Secret Sharing Scheme [6]
An extension to Shamir’s secret sharing scheme is published by Thien and Lin in 2002, in which when the secret data using secret sharing scheme is an image, then the secret image will be divided into \( n \) pieces of shadow images which in a smaller size of the secret image.

Image secret sharing is using a polynomial of degree \( k - 1 \) to generate \( n \) pieces of shadow images from secret image with \( m \times m \) pixels. The pixel value is denoted by \( I \). Since the grey level from a pixel value is between 0 and 255, then a prime number \( p = 251 \) will be used for later, where 251 is the biggest prime number on the range of the grey level. The polynomial is \( q(x) = a_0 + a_1 x + \cdots + a_{k-1} x^{k-1} \), where \( D = a_0 \), and \( D_1 = q(1), \ldots, D_i = q(i), \ldots, D_n = q(n) \), with each piece of \( D_i \) is a shadow image. In this method, the size of the shadow images is \( 1/k \) of secret image.

2.3. Li Bai’s Secret Sharing Scheme using Matrix Projection [11]
Li Bai developed \((k, n)\) threshold Shamir by representing the secret data into square matrix \( S \), and the secret matrix will be shared to all participants using matrix projection. The advantage of this scheme is the secret data is more protected. For an \( m \times k \) matrix \( A \) with rank \( k \) \((m \geq k > 0)\), an \( m \times m \) matrix \( S \) is matrix projection of matrix \( A \), with \( S = A(A^T A)^{-1} A^T \) or denoted by \( S = \text{proj} (A) \).

2.4. Li Bai’s Image Secret Sharing Scheme using Matrix Projection [2]
In the same year, Li Bai developed an image secret sharing, where this method divides a secret colour image into \( n \) pieces of image shares such that any \( k \) image shares will be able to reconstruct the secret image. This image secret sharing scheme is using Thien and Lin’s image secret sharing, in which the main essence is using a polynomial of degree \( k - 1 \) to construct \( n \) image shares from an \( m \times m \) secret image, with the pixel value denoted by \( I \).

The polynomial can be written as follows:

\[
S_{lt}(c) = I(i, k(t-1)+1) + I(i, k(t-1)+2) + \cdots + I(i, k(t-1)+k) c_j^{k-1} \mod 251
\]

where \( 1 \leq t \leq \left\lceil \frac{m}{k} \right\rceil \) dan \( 1 \leq i \leq m \).

In this method, the size of image shares is \( 1/k + 1/m \) of secret image.

2.5. Verifiable Secret Sharing Scheme
Verifiable Secret Sharing Scheme is a cryptographic protocol in which its existence ensures each participant could verify their received piece of share without knowing the secret [3].

Wang proposed verification method in secret sharing scheme in which an \( n \times n \) watermark image will be used with the secret image to construct shadow images. The accuracy of watermark image will determine the reliability from shadow images before reconstructing the secret image. If the reconstructed image using watermark image accurate, then the reconstructed shadow images is also proven to be accurate. Therefore, the secret image could be verified [7].

3. Verifiable Image Secret Sharing Scheme using Matrix Projection
The problem with reliable secret sharing scheme using matrix projection published by Li Bai is they do not provide a way for participants to validate their received image shares, where as there is a possibility of a disturbance in transmission or problem that come off by dealing with dishonest dealers or shareholders. An extension to secret sharing scheme developed by Wang et al. in which an \( m \times m \)
watermark image will be shared with image shares, and by determining the accuracy of watermark image, then the reconstructed secret image could be verified.

This paper will modify the image secret sharing scheme using matrix projection by Li Bai with the use of the watermark image in Wang et al.’s scheme to resolve the problem stated above.

The scheme is presented as below.

3.1. Construct Image Shares
- Determine the \((k, n)\) threshold and the matrix of secret image \(S\)
- Construct a random \(m \times k\) matrix \(A\) of rank \(k\) where \(m > 2 (k - 1) - 1\)
- Calculate projection matrix \(S = proj(A) \mod p\) and remainder matrix \(R = (S - S) \mod p\)
- Choose \(n\) of \(k\) random vector \(x_j\), and no \(c_j\) for \(1 \leq j \leq n\)
- Compute share vector \(v_j = (Ax) \mod p\) for \(1 \leq j \leq n\), \(p\) is a prime number
- Use Thien and Lin image secret sharing, the remainder matrix \(R\) is used to create shares as follows:
  \[ G_j = [g_1^{(j)} g_2^{(j)} \cdots g_{m+k}^{(j)}] \]
  in which \(g_i^{(j)} = (I(i, 1) + 1) + \cdots + I(i, k(t - 1) + k) c_j^{k-1} \mod 251\)
- Select watermark image \(W\) and compute remainder matrix \(R_w = (W - S) \mod p\)
- Divide image shares \(Sh_j = [v_j G_j]\) to participants and make matrix \(R_w\) public

3.2. Reconstruct Secret Image
- Select \(k\) image shares from any \(k\) participants, namely \(Sh_1, Sh_2, \ldots, Sh_k\)
- Construct remainder matrix \(R\) using Thien and Lin and compute \(B = [v_1 v_2 \cdots v_k]\)
- Compute projection matrix \(S = (proj(B)) \mod p\)
- Construct remainder matrix \(R\) using Thien and Lin image secret sharing, by using \(G_j\) as follows:
  \[ R = \begin{bmatrix}
  r_1^{(1)} & r_2^{(1)} & \cdots & r_y^{(1)} \\
  r_1^{(2)} & r_2^{(2)} & \cdots & r_y^{(2)} \\
  \vdots & \vdots & \ddots & \vdots \\
  r_1^{(x)} & r_2^{(x)} & \cdots & r_y^{(x)}
  \end{bmatrix} \]
  in which \(r_y^{(x)} = [I(x, k(y - 1) + 1) \quad I(x, k(y - 1) + 2) \quad \cdots \quad I(x, k(y - 1) + k)]\)
  where \(1 \leq x \leq m\), dan \(1 \leq y \leq \left\lceil \frac{m}{k} \right\rceil\)
- Calculate secret image \(S = (S + R) \mod p\)
- Determine value of watermark image \(W = ((S + R_w) \mod p)\)
- Divide image shares \(Sh_j = [v_j G_j]\) to participants and make matrix \(R_w\) public

3.3. Example
For further understanding, given the examples of construction and reconstruction process below.
- Choose secret image \(S\), and \((2, 4)\) threshold scheme, with \(p = 251\) and construct random matrix \(A\).
  \[
  \text{Let } S = \begin{bmatrix} 2 & 5 & 2 & 3 \\ 3 & 6 & 4 & 5 \\ 4 & 7 & 4 & 6 \\ 1 & 4 & 1 & 7 \end{bmatrix} \quad \text{and } A = \begin{bmatrix} 3 & 7 \\ 6 & 1 \\ 2 & 5 \\ 6 & 6 \end{bmatrix}.
  \]
- Calculate the matrix projection \(S\) using the formulas stated above.
Using calculations above, matrix share
Say
Select watermark image

\[ g \]

For \( g \)

For \( g \)

Then, calculate remainder matrix

\[ R = (S - S)(mod \ p) = \begin{bmatrix}
1 & 221 & 201 & 214 \\
221 & 189 & 186 & 16 \\
201 & 186 & 43 & 76 \\
214 & 16 & 76 & 20 \\
\end{bmatrix} \]

After that, choose 4 vectors \( x_j \) with size 2 \times 1, and 4 values of \( c_j \) with \( 1 \leq j \leq 4 \)

\[ x_1 = [9], \quad x_2 = [4], \quad x_3 = [9], \quad x_4 = [3] \]

and \( c_1 = 1, \ c_2 = 2, \ c_3 = 3, \ c_4 = 4 \)

Compute share vector

\[ v_j = (Ax_j)(mod \ p) \text{ for } 1 \leq j \leq 4 \]

\[ v_1 = [62], \quad v_2 = [40], \quad v_3 = [83], \quad v_4 = [23] \]

Use Thien and Lin image secret sharing with the remainder matrix \( R \) is used to create shares as follows:

\[ G_j = [g_1^{(j)}, g_2^{(j)}, \ldots, g_{m}^{(j)}] \]

For \( t = 1 \Rightarrow g_1^{(j)}(i) = (I(i, 1) + I(i, 2) c_j) \mod 251 \)

For \( t = 2 \Rightarrow g_2^{(j)}(i) = (I(i, 3) + I(i, 4) c_j) \mod 251 \)

For \( j = 1 \Rightarrow G_1 = [g_1^{(1)}], \quad j = 3 \Rightarrow G_3 = [g_1^{(3)}] \]

\[ G_2 = [g_2^{(1)}], \quad G_4 = [g_1^{(4)}, g_2^{(4)}] \]

Calculate \( G_1 \):

\[ g_1^{(1)}(i) = (I(i, 1) + I(i, 2) c_1) \mod 251, \text{ and } g_2^{(1)}(i) = (I(i, 3) + I(i, 4) c_1) \mod 251 \]

For \( i = 1 \):

\[ g_1^{(1)}(1) = (I(1, 1) + I(1, 2) c_1) \mod 251 = (1 + 35(1)) \mod 251 = 36 \mod 251 = 36 \]

\[ g_2^{(1)}(1) = (I(1, 3) + I(1, 4) c_1) \mod 251 = (52 + 40(1)) \mod 251 = 92 \mod 251 = 92 \]

Following the same pattern for \( i = 2, 3, 4 \), the value will be obtained as follows:

\[ g_1^{(1)}(2) = 101, \quad g_2^{(1)}(2) = 58, \quad g_1^{(1)}(3) = 126, \quad g_2^{(1)}(3) = 142, \]

\[ g_1^{(1)}(4) = 26, \quad g_2^{(1)}(4) = 163 \]

Thus, the matrix \( G_1 = \begin{bmatrix} 36 & 92 \\ 101 & 58 \\ 126 & 142 \\ 26 & 163 \end{bmatrix} \)

Using the same steps, the matrices will be obtained as follows:

\[ G_2 = \begin{bmatrix} 71 & 132 \\ 169 & 47 \\ 198 & 72 \\ 14 & 150 \end{bmatrix}, \quad G_3 = \begin{bmatrix} 106 & 172 \\ 237 & 36 \\ 19 & 2 \\ 2 & 137 \end{bmatrix}, \quad G_4 = \begin{bmatrix} 141 & 212 \\ 54 & 25 \\ 91 & 183 \\ 241 & 124 \end{bmatrix} \]

Select watermark image \( W \) and compute remainder matrix \( R_w = (W - S)(mod \ p) \)

| 50 | 100 | 21 | 14 |
|----|-----|----|----|
| 22 | 76  | 200| 54 |
| 1  | 91  | 45 | 7  |
| 24 | 66  | 96 | 120|

\[ R_w = \begin{bmatrix} 49 & 130 & 71 & 51 \\ 52 & 138 & 14 & 38 \\ 51 & 156 & 2 & 182 \\ 61 & 50 & 20 & 100 \end{bmatrix} \]

Using calculations above, matrix share \( Sh_j = [v_j \ G_j] \) for \( j = 1, 2, 3, 4 \) is obtained as follows:

\[ Sh_1 = [62 \ 36 \ 92], \quad Sh_2 = [40 \ 71 \ 132], \quad Sh_3 = [83 \ 106 \ 172], \quad Sh_4 = [23 \ 141 \ 212] \]

\[ Sh_1 = [59 \ 101 \ 58], \quad Sh_2 = [28 \ 169 \ 47], \quad Sh_3 = [62 \ 237 \ 36], \quad Sh_4 = [20 \ 54 \ 25] \]

\[ Sh_1 = [43 \ 126 \ 142], \quad Sh_2 = [28 \ 198 \ 72], \quad Sh_3 = [58 \ 19 \ 2], \quad Sh_4 = [16 \ 91 \ 183] \]

\[ Sh_1 = [84 \ 26 \ 163], \quad Sh_2 = [48 \ 14 \ 150], \quad Sh_3 = [102 \ 2 \ 137], \quad Sh_4 = [30 \ 241 \ 124] \]
Image share $S_{h_1}$ will be shared to participant 1, image share $S_{h_2}$ will be shared to participant 2, and so on. Remainder matrix $R_w$ will be a public share.

- Select 2 image shares from $S_{h_1}, S_{h_2}$
  
  $$
  S_{h_1} = \begin{bmatrix}
  62 & 36 & 92 \\
  59 & 101 & 58 \\
  43 & 126 & 142 \\
  84 & 26 & 163
  \end{bmatrix}, \quad S_{h_2} = \begin{bmatrix}
  40 & 71 & 132 \\
  28 & 169 & 47 \\
  28 & 198 & 72 \\
  48 & 14 & 150
  \end{bmatrix}
  $$

- Construct matrix $B$ using first column of share 1 and share 2, such that $B = [v_1 \quad v_2]$.
  
  $$
  v_1 = \begin{bmatrix}
  62 \\
  59 \\
  43 \\
  84
  \end{bmatrix}, \quad v_2 = \begin{bmatrix}
  40 \\
  28 \\
  28 \\
  48
  \end{bmatrix}, \quad B = \begin{bmatrix}
  62 & 40 \\
  59 & 28 \\
  43 & 28 \\
  84 & 48
  \end{bmatrix}
  $$

- Compute matrix projection $S = (\text{proj}(B))(\text{mod} \ p)$
  
  $$
  S = \begin{bmatrix}
  1 & 221 & 201 & 214 \\
  221 & 189 & 186 & 16 \\
  201 & 186 & 43 & 76 \\
  124 & 16 & 76 & 20
  \end{bmatrix}
  $$

- Construct matrix $G$ with elements from share 1 and 2 without the first column
  
  $$
  G_1 = \begin{bmatrix}
  36 & 92 \\
  101 & 58 \\
  126 & 142 \\
  26 & 163
  \end{bmatrix}, \quad G_2 = \begin{bmatrix}
  71 & 132 \\
  169 & 47 \\
  198 & 72 \\
  14 & 150
  \end{bmatrix}
  $$

Then, use $G$ to construct remainder matrix $R$ with formulas stated before.

$$
\begin{align*}
  r_j(x) &= [I(x, k(y-1) + 1) \quad I(x, k(y-1) + 2)] \\
  \text{In which value of} \ x \text{obtained using Gauss-Jordan from:}
  \end{align*}
$$

$$
\begin{bmatrix}
  1 & c_1 \\
  1 & c_2 \\
  \vdots & \vdots \\
  1 & c_j
\end{bmatrix}
\begin{bmatrix}
  I(x, 2(y-1) + 1) \\
  I(x, 2(y-1) + 2)
\end{bmatrix} =
\begin{bmatrix}
  G_1(x, y) \\
  G_2(x, y)
\end{bmatrix} \text{ (mod) p}
$$

where $1 \leq c_1 = j \leq 2, 1 \leq x \leq 4, \text{ and } 1 \leq y \leq 2$

$$
\begin{align*}
  &x = 1: \text{For } y = 1, \quad G_1(1,1) = 36, \quad G_2(1,1) = 71 \\
  &\begin{bmatrix}
  1 \\
  2
\end{bmatrix}
\begin{bmatrix}
  I(1,1) \\
  I(1,2)
\end{bmatrix} = \begin{bmatrix}
  36 \\
  71
\end{bmatrix} \text{ (mod) 251} \Rightarrow \begin{bmatrix}
  1 & 35 \\
  0 & 1
\end{bmatrix} \Rightarrow \text{So, } r_1^{(1)} = [1 \quad 35]
\end{align*}
$$

$$
\begin{align*}
  &x = 2: \text{For } y = 2, \quad G_1(1,2) = 92, \quad G_2(1,2) = 132 \\
  &\begin{bmatrix}
  1 \\
  2
\end{bmatrix}
\begin{bmatrix}
  I(1,3) \\
  I(1,4)
\end{bmatrix} = \begin{bmatrix}
  92 \\
  132
\end{bmatrix} \text{ (mod) 251} \Rightarrow \begin{bmatrix}
  1 & 52 \\
  0 & 1
\end{bmatrix} \Rightarrow \text{So, } r_2^{(1)} = [52 \quad 40]
\end{align*}
$$

Following the same pattern, the value will be determined as follows:

$$
\begin{align*}
  &r_1^{(2)} = [33 \quad 68] \quad \quad \quad r_1^{(3)} = [54 \quad 72] \quad \quad \quad r_1^{(4)} = [38 \quad 239] \\
  &r_2^{(2)} = [69 \quad 240] \quad \quad \quad r_2^{(3)} = [212 \quad 181] \quad \quad \quad r_2^{(4)} = [176 \quad 238]
\end{align*}
$$

Thus, the remainder matrix $R = \begin{bmatrix}
  1 & 35 & 52 & 40 \\
  33 & 68 & 69 & 240 \\
  54 & 72 & 212 & 181 \\
  38 & 239 & 176 & 238
\end{bmatrix}$

- Construct secret matrix $S = (S + R) \text{ (mod) p}$ and Verify using watermark image $W$, calculate
  $$
  W = ((S + R_w) \text{ (mod) p})
  $$

$$
\begin{align*}
  S = \begin{bmatrix}
  2 & 5 & 2 & 3 \\
  3 & 6 & 4 & 5 \\
  4 & 7 & 4 & 6 \\
  1 & 4 & 1 & 7
\end{bmatrix} \text{ and } W = \begin{bmatrix}
  50 & 100 & 21 & 14 \\
  22 & 76 & 200 & 54 \\
  1 & 91 & 45 & 7 \\
  24 & 66 & 96 & 120
\end{bmatrix}
\end{align*}
$$
As stated above, the proposed scheme constructs image shares by the secret image itself, and the watermark image will use the same projection matrix to build a public matrix. Afterward, the image shares are used to reconstruct the secret image, and the public matrix is used to determine the watermark image. Then, verify the accuracy of the watermark image using PSNR. An expected result would show high PSNR values, which show the accuracy of the watermark image, and so does the reconstructed secret image. If the watermark image is accurate, then the reconstructed secret image is accurate and valid.

4. Result and Implementation
Using the algorithm stated above, with (2, 4) threshold scheme, Figure 1 shown the secret image S, and Figure 2 shows the watermark image W. Each figure is in size 256 × 256 pixels.

Figure 3-6 below was image shares obtained by using the construction process, with each size of the image shares are 256 × 129 pixels. Figure 3 was representing image share 1, figure 4 was representing image share 2, and so on.

5. Conclusion
In order to prevent dishonest dealer and provide a way for participants to validate their received image share, this paper presented a verifiable image secret sharing scheme using matrix projection, in which the matrix projection was used to create image shares and a public matrix from watermark image. The watermark image was used for verifiability, where the reconstructed watermark image verifies the accuracy of the reconstructed secret image.

6. References
[1] Bai L 2006 A Strong Ramp Secret Sharing Scheme Using Matrix Projection Proc. of The 2006 Int. Symp. On a World of Wireless, Mobile and Multimedia Networks (Washington DC: IEEE Computer Society) pp 652-656
[2] Bai L 2006 A Reliable (k, n) Image Secret Sharing Scheme 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing (Philadelphia: IEEE Computer Society) pp 31-36
[3] Chor B, Goldwasser S, Micali S, Awerbuch B 1985 Verifiable Secret Sharing and Achieving Simultaneity in the Presence of Faults 26th Annual Symp. on Found. of Comp. Sci., pp 383-395
[4] Ridayanti F 2013 Skemapembagian Data Rahasia yang Menggunakan Matriks Proyeksipada Citra Digital (Skripsi) Fakultas Matematikad dan Ilmu Pengetahuan Alam Universitas Indonesia
[5] Shamir A 1979 How to share a secret Communications of the ACM 22(11) pp 612–613
[6] Thien C C and Lin J C 2002 Secret image sharing Computers & Graphics 26(5) pp 765-770
[7] Wang Z H, Chang C C, Tu H N, and Li M C 2010 Journals of Informations Hiding and Multimedia Signal Processing 2(1) pp 78-90

Acknowledgments
Part of this research was funded by PITTA-UI 2018 Research Grant [Project Number = 2277/UN2.R3.1/HKP.05.00/2018].