A novel scheme for lossless authenticated multiple secret images sharing using polynomials and extended visual cryptography

Krishnaraj Bhat¹ | Uday Kumar Reddy K.R.¹ | Ranjan Kumar H.S.¹ | Dindayal Mahto²

¹Department of Computer Science and Engineering, NMAM Institute of Technology, Nitte, Karnataka, India
²Department of Information Technology, School of Computing, SASTRA Deemed to be University, Thanjavur, Tamil Nadu, India

Correspondence
Krishnaraj Bhat, Department of Computer Science and Engineering, NMAM Institute of Technology, Nitte, Karnataka, 574110, India.
Email: krishvaradha08@gmail.com

Abstract
Researchers have put forward many variations of schemes for secret image sharing on grounds of visual cryptography and polynomials. The authors of this paper put forward a novel scheme for sharing multiple secret images with perfect reconstruction and authentication for cheating prevention. The perfect reconstruction of all shared secret images is obtained by applying polynomial-based encryption and decryption, and one-time authentication is done for all shared secret images by stacking the intelligible shares created by using extended visual cryptography. Properties' analysis, experimental results and comparisons are given to exhibit the potency of the scheme.

1 | INTRODUCTION

Naor and Shamir [1] proposed the (v, z) – visual cryptography scheme (VCS) – where a secret image is divided into z noisy images called shares or shadows, and issued to z participants. A minimum of v shares from v participants are stacked to visually decrypt the original secret image. The beauty of this scheme is that it does not require a key to perform encryption or decryption, and even though z−v shares are absent, the secret images can be revealed. As the shares are unintelligible, they get the attention of attackers and become vulnerable to attacks while being transmitted in an open network. To overcome this issue, an extended visual cryptography scheme (EVCS) [2] is proposed in which shares are made intelligible besides reconstructing the original secret using the intelligible shares.

Cheating prevention methods in (v, z)–VCS with respect to different kinds of cheating and cheaters are proposed in [3–5]. Hu and Tzeng [3] proposed three cheating approaches in VCS and EVCS, and a general method for transforming a VCS into a different VCS which has got the cheating prevention feature is also proposed. Each participant contains a verification share for authenticating other participants' shares. They also proposed betterments on previous cheating prevention schemes. Ren et al. [4] proposed a cheating prevention method where each participant has a verification share created by using Latin square to authenticate other participants' shares supporting both deterministic VCS and probabilistic VCS. Kumar et al. [5] proposed cheating prevention by using remedial number system (RNS) and mixed radix representation (MRR) for encryption and decryption, respectively, supporting only (v, v)–image secret sharing (ISS). It does not discuss how the moduli values used in RNS and MRR are shared among participants.

Two-in-one ISS (TiOISS) schemes, where low-quality secret image is revealed in the first phase of decoding and high-quality secret image is recreated in the second phase of decoding, are proposed in [6–13]. Schemes in which stacking is used in the first phase of decoding and Lagrange's interpolation in the second phase are proposed in [6–9,11,13]. Li et al. [10] proposed the first-phase decoding using stacking and the second-phase decoding using few XOR operations. The secret image has to be resized if its half-toned image does not have adequate black pixels. The size of shares depends on the number of black pixels, pixel expansion and number of grey values greater than 253 in the secret image. Chen et al. [11] combined polynomial image secret sharing (PISS) and random grid-based visual secret sharing (RGVSS), where the size of shares is the same as that of secret image. Sridhar [12] proposed a scheme for sharing multiple secret images in which low-quality secret images are recreated in the first phase of decoding by stacking the circular shares which are rotated in counter-clockwise direction at different angles, respectively. A truncation of PISS pixels is done before embedding them into visual multiple-secret sharing (VMSS) to improve share's visual quality due to which revealed secret images after the second phase of decoding is not the same.
as original secret images. There is a constraint on the size of the secret images in which PSIS shadows have to be created with respect to threshold $\mathcal{V}$ and radius of circular shares. Also, there is an extra burden of carrying a number of PSIS pixels and authentication bits in shares. Wu and Yang [13] proposed a scheme in which a greyscale secret image is converted into $p$-radix image from which $z$ $p$-radix shares are obtained by $(v, z)$–PSIS under mod $p$ operation. Then these generated $p$-radix shares are embedded into colour shares using colour shares generation algorithms which are needed to recreate the secret image in lossless form after decryption. Again a secret image is half-toned and shared using $z$ colour shares formed by applying $(v, z)$ colour black white (CBW)–VCS which can be decoded by stacking. Among these, only Srividhya et al. [9] and Sridhar and Sudha [12] support authentication of intelligible shares with respect to a malicious attacker from outside.

Schemes for sharing multiple secrets at a time are proposed in by Chang et al. [14], Nitharwal and Verma [15], Ovhal et al. [16], Deshmukh et al. [17], Sasaki and Watanabe [18], Kabirirad and Eslami [19], Kapadiya et al. [20], and Prasetyo and Guo [21]. Chang et al. [14] proposed sharing multiple secret images using the Chinese Remainder Theorem (CRT) and Lagrange's interpolation. Each shared pixel produced can have a value greater than 255 which needs more than a byte memory to get accommodated, and no mean for identifying these shared pixel values greater than 255 is proposed. Nitharwal and Verma [15] and Ovhal et al. [16] proposed sharing multiple secret images supporting only $(v, z)$ ISS where the number of shares $z$ produced is equal to the number of secret images shared. Nitharwal and Verma [15] used XOR and bit-reversal operations, whereas Ovhal et al. [16] used modulo addition and subtraction, XOR and bit-reversal operations. Deshmukh et al. [17] utilised CRT and XOR operations to share multiple secret images where the number of shares $z$ produced is equal to the number of secret images shared. When the number of secret images to be shared is odd, it is not able to reconstruct recovered secret images correctly. Sasaki and Watanabe [18] provided adequate conditions to be satisfied by encryption of visual secret sharing scheme actualising a general form of access structure for multiple secrets and two constructions of such scheme with encryption fulfilling the condition. Kabirirad and Eslami [19] proposed sharing multiple secret images using XOR, reverse and cyclic shift operations, where $v$ consecutive shares are required to reconstruct the secret images. The number of secret images that can be shared at a time is $v$, where $v$ being the threshold in $(v, z)$–multiple secret image sharing scheme. Kapadiya et al. [20] proposed sharing multiple secret images using XOR operation. To share $z$ secret images, $z + 1$ shares are generated among which one is a universal share, and shares are created in order starting from the universal share. To retrieve all $z$ secret images, all $z + 1$ shares are required. But, to retrieve secret images individually, all shares are not required. To recover the first secret image, the universal share and the second share are sufficient. To recover the second secret image, the universal share, the second share and third share are required, and so on. Exact recovery of the secret images is not done. But, they are visually alike original ones. Prasetyo and Guo [21] overcome the limitation of Deshmukh et al. [17] with respect to odd numbers of secret images. It is done by introducing symmetric and transferred masking coefficients to produce a set of shared images. To further improve security, hyper-chaotic scrambling is used to transpose the secret images ahead of generating shared images.

The existing schemes briefed so far have the following limitations: (i) identification and management of shares are difficult due to their noisy nature [1,4–8,10,11,13–19,21]; (ii) extra verification shares are generated for authentication which consume extra storage space [14,15,17]; (iii) difficult to find the reference points of rotation for shares carrying multiple secret images data [12]; (iv) shares have to be circumvented in a specific way to reconstruct each of the multiple secret images [12]; (v) support only $(v, v)–$ ISS for $v \geq 2$ [5,15–17,20,21]; (vi) the number of shares to be created is dependent on the number of secret images to be shared [15–17,20,21]; and (vii) need of ordered consecutive shares to recover the secret images [15–17,19–21]. In addition to overcoming the above-mentioned limitations, the proposed scheme has other advantages as follows: (i) maximum of $m/2$ secret images are shared using $z$ shares, $m$ being the pixel expansion, (ii) lossless recovery of all $m/2$ secret images using at least $v$ shares; (iii) only one-time authentication for the recovering of all $m/2$ shared secret images; and (iv) resistant to different kinds of cheating and cheaters mentioned in [3].

The rest of the article is organized as follows. Section 2 briefs preliminaries utilised in the scheme proposed. Sections 3 and 4 describe the scheme proposed and provide analysis on the properties of the scheme, respectively. Section 5 delivers the results of experiments and comparison details. Section 6 provides conclusion and future work details, and references, respectively.

## 2 | PRELIMINARIES

### 2.1 | $(v, z)–$Visual Cryptography Scheme

A secret image is segregated into $z$ shares by the dealer using $(v, z)–$VCS, $2 \leq v \leq z$. To reveal the secret image, at least $v$ shares have to be stacked. Any less than $v$ shares cannot disclose the secret image. A $(v, z)–$VCS is defined as follows [1]:

**Definition 1** $(v, z)–$VCS comprises two accumulations $Q_0$ and $Q_1$ of $z \times m$ Boolean matrices, $m$ is the pixel expansion. If the following two requirements hold, then the scheme is considered legitimate:

i. By stacking any $v$ rows in $\mathcal{W} \in Q_0$, the count of white (black) pixels in the resulting vector should be greater (lesser) than the count of white (black) pixels in the resulting vector that is got by stacking any $v$ rows in $\mathcal{B} \in Q_1$.

ii. By stacking any $j$ rows, $1 \leq j < v$, in $\mathcal{W} \in Q_0$, the count of white (black) pixels in the resulting vector should be the same as the count of white (black) pixels in the resulting vector that is got by stacking any $j$ rows in $\mathcal{B} \in Q_1$.

Requirement 1 is in respect of the contrast of the revealed secret image and requirement 2 is in respect of the security of
the scheme that makes sure that by stacking any less than \( \nu \) shares, only unintelligible image is revealed. Figure 1 depicts the \((2, 2)\)-VCS. It can be seen that shares 1 and 2 are noisy, revealing no information about secret. But on stacking, secret is revealed. ‘4’ denotes stacking operation.

### 2.2 \((\nu, z)\)-extended visual cryptography scheme

**Definition 2** Let \( \{(Q^h_w, \ldots, Q^h_b), \ldots, (Q^h_{z-1}w, \ldots, Q^h_z b)\}_{b_1, \ldots, b_{\nu} \in \{w, b\}} \) be a couple of \( 2^\nu \) collections of \( z \times m \) Boolean matrices forming a \((\nu, z)\)-EVCS, if there exist values \( r_1, r_2 \) and \( t \) satisfying the following:

1. For \( b_1, \ldots, b_{\nu} \in \{w, b\} \), the threshold \( t \) and the relative difference \( r_1 \) are such that, for any \( M \in \mathbb{Q}^{h_1, \ldots, h_{\nu}} \), the OR \( K \) of any \( v \) of the \( \nu \) rows satisfies \( H(K) \leq t \times r_1 \times m \); whereas, for any \( M \in Q^{h_1, \ldots, h_{\nu}} \), \( H(K) \geq t \).

2. For any \( b_1, \ldots, b_{\nu} \in \{w, b\} \) and for any subset \( \{x_1, \ldots, x_p\} \in \{1, \ldots, z\} \) with \( p < \nu \), the two collections of \( p \times m \) matrices \( R^{h_1, \ldots, h_{\nu}}_{p} \) with \( d \in \{w, b\} \) obtained by restricting each \( z \times m \) matrix in \( Q^{h_1, \ldots, h_{\nu}} \) to rows \( x_1, \ldots, x_p \) contain the identical matrices with the same number of occurrences.

3. For any \( x \in \{1, \ldots, z\} \) and any \( b_1, \ldots, b_{\nu-1}, b_{\nu+1}, \ldots, b_{\nu} \in \{w, b\} \), it results that \( \min H(M_x)_{M \in \mathbb{Q}^{h_1, \ldots, h_{\nu}}} \geq r_2 \times m \),

where

\[
\mu_w = \bigcup_{b_1, \ldots, b_{\nu-1}, b_{\nu+1}, \ldots, b_{\nu} \in \{w, b\}} Q^{h_1, \ldots, h_{\nu-1}b_{\nu+1}, \ldots, b_{\nu}}
\]

\[
\mu_b = \bigcup_{b_1, \ldots, b_{\nu-1}, b_{\nu+1}, \ldots, b_{\nu} \in \{w, b\}} Q^{h_1, \ldots, h_{\nu-1}b_{\nu+1}, \ldots, b_{\nu}}
\]

The values \( r_1 \) and \( r_2 \) are relative difference of the revealed image and relative difference of the shares, respectively; \( m \) is the pixel expansion; and \( H(K) \) is the vector \( K \)'s hamming weight.

Requirement 1 is in respect of contrast of the revealed secret image and requirement 2 is in respect of the security of the scheme where less than \( \nu \) shares cannot reveal any details about secret on stacking. Requirement 3 implies that the meaning of original image in the share is not modified. Figure 2 depicts the \((2, 2)\)-EVCS, where it is shown that shares 1 and 2 are intelligible, revealing no details about the secret image individually.

### 2.3 \((\nu, z)\)-polynomial image secret sharing scheme

Shamir [22] first proposed \((\nu, z)\) PISSS for dividing a secret into \( \nu \) shares and obtain the secret back by using \( \nu \) shares. Thien and Lin [23] proposed an improvement on [22], where the size of shares is \( \nu \) times smaller than that of secret image. The operations are carried out under mod 251. As pixel values scale from 0 to 255, the values above 250 are truncated to 250. This caused loss of information in the reconstructed secret image. But, this problem is overcome by performing operations under GF \((2^8)\), where GF stands for the Galois field.

Zhou et al. [24] took two adjacent pixels in the secret image as one unit which can have the values in the range [0, 65,535]. If 65,536 is obtained as the value of shared pixel by Lagrange’s interpolation under prime modulus 65,537, then encryption operation is repeated unless a value in the range [0, 65,535] is obtained. Also, it requires that the number of pixels in secret image to be even. We use GF \((2^8)\) operations in our proposed scheme.

Polynomial equations (1) and (2) are used for encryption and decryption, respectively, and Equation (2) is Lagrange’s interpolation formula:

\[
L(u) = (s_0 + s_1u + s_2u^2 + \ldots + s_{\nu}u^{\nu-1}) \mod GF(2^8),
\]

\[
L(u) = (\sum_{i=1}^{\nu} (c_i \times b_i)) \mod GF(2^8),
\]

where

\[
b_i = \prod_{1 \leq j \leq \nu, j \neq i} \left( \frac{u - y_j}{y_i - y_j} \right)
\]

In Equation (1), \( L(u) \) is the polynomial of degree \( \nu-1 \) and \( s_i \), \( 0 \leq i \leq \nu-1 \), are \( \nu \) secret values. In Equation (2), \( c_i, 1 \leq i \leq \nu \), are the \( \nu \) cipher values obtained for \( \nu \) different \( u \) values in

![Figure 1](image1.png)

**Figure 1** (2, 2)-VCS: (a) secret image, (b) share 1, (c) share 2 and (d) revealed secret image (share 1 + share 2)

![Figure 2](image2.png)

**Figure 2** (2, 2) – EVCS: (a) secret image, (b) share 1, (c) share 2, and (d) revealed secret image (share 1 + share 2)
Equation (1). It is possible to obtain more than \( v \) cipher values for the same \( v \) secret values. But, at least, \( v \) cipher values are required to retrieve the original \( v \) secret values.

### 2.4 | Digital half-toning

Digital half-toning is the transformation of a greyscale image into a binary image containing black and white pixels only. As most of the VCS and EVCS schemes work with black and white pixels, secret images in the greyscale form are converted into black and white images. In our proposed scheme, we apply the widely used Floyd–Steinberg error diffusion technique for half-toning.

In this technique, 43.75%, 18.75%, 31.25% and 6.25% of the error calculated at a pixel position \((f, g)\) are transferred to unprocessed pixels at positions \((f, g + 1)\), \((f + 1, g - 1)\) \((f + 1, g)\) and \((f + 1, g + 1)\), respectively. Figure 3 shows half-toned version of a colour image obtained by applying the Floyd–Steinberg half-toning to each red, green and blue (RGB) component of a rainbow colour image.

### 3 | PROPOSED \((v, z)\)–LAMSIS SCHEME

In this section, the proposed \((v, z)\)–LAMSIS (lossless authenticated multiple secret images sharing) scheme consists of two parts: encryption and decryption with an example is described. The \((v, z)\)–LAMSIS scheme can be used on binary, greyscale and colour images. The encryption and decryption are done by the dealer.

#### 3.1 | Encryption

**Input:** \( v \) intelligible shares \( S_1, S_2, \ldots, S_v \).

**Output:** \( z \) meaningful shares \( S_1, S_2, \ldots, S_z \).

![Figure 3](image)

**Figure 3** Half-toning: (a) original image and (b) half-toned image

Step 1: Half-tone \( A \), and each \( C_i \) to get \( HA \) and \( HC_i \), \( 1 \leq i \leq z \), HA and HC are the half-toned authentication image and half-toned cover images, respectively.

Step 2: Using \((v, z)–EVCS\), obtain the intermediate shares \( S_{1}, S_{2}, \ldots, S_{v} \) by using HC, \( 1 \leq i \leq z \) as cover images and HA as the secret image.

Step 3: Read \( v \) consecutive pixels from each \( SI_{j} \) and store them in \( s_{ij} \) for each \( SI_{j} \), \( 1 \leq i \leq v \) and \( 1 \leq j \leq r \).

Step 4: Substitute these \( v \) secret values \( s_{ij} \) in (1) and compute \( z \) cipher values \( c_{kj} \) for each \( SI_{j} \), \( 1 \leq x \leq z \).

Step 5: Express \( c_{kj} = q_{kj} \times 16 + p_{kj} \), where \( q_{kj} \) and \( p_{kj} \) are the quotient and the remainder obtained on dividing \( c_{kj} \) by 16, respectively.

Step 6: Read corresponding block of \( m \) pixels from each share \( S_{x} \), \( 1 \leq x \leq z \) and find the positions of the first \( r \) black pixels and \( r \) free pixels.

Step 7: Store \( q_{kj} \), \( 1 \leq j \leq r \), values in least four bits of \( r \) black pixels and \( p_{kj} \) values in least four bits of \( r \) free pixels in order.

Step 8: Iterate from Step 3 to Step 7 unless all the pixels in \( r \) secret images are processed.

Here, the authentication image is known only to the dealer and each participant chooses his/her own cover image. Free pixels are those pixels in a block other than the first \( r \) black pixels and \( r = m/2 \).

#### 3.2 | Decryption

**Input:** \( v \) intelligible shares \( S_1, S_2, \ldots, S_v \).

**Output:** \( r \) reconstructed secret images \( SI_{1}, SI_{2}, \ldots, SI_{r} \) on successful authentication.

Step 1: Stack the \( v \) shares \( S_i, 1 \leq i \leq v \), to check whether the authentication image is reconstructed. If yes, proceed to Step 2. Else, cheating is detected and reconstruction of secret images is stopped.

Step 2: Read block of \( m \) pixels from each share \( S_{x} \), \( 1 \leq x \leq v \), and find the positions of the first \( r \) dark grey pixels and remaining \( r \) pixels.

Step 3: Retrieve \( q_{kj} \), \( 1 \leq j \leq r \), values from the least four bits of first \( r \) dark grey pixels and \( p_{kj} \) values from the least four bits of the remaining \( r \) pixels.

Step 4: Compute cipher values \( c_{kj} \) as \( c_{kj} = q_{kj} \times 16 + p_{kj} \).

Step 5: Substitute these \( v \) cipher values in Equation (2) to get \( v \) corresponding secret values for each \( j, 1 \leq j \leq r \) which are stored in corresponding locations of secret images being reconstructed.

Step 6: Iterate from Step 2 to Step 5 unless all the blocks in the \( v \) shares are processed.

#### 3.3 | Example

We illustrate our proposed scheme for one block with \( v = 2 \) and \( z = 2 \). Here, pixel expansion \( m = 4 \) and \( r = m/2 = 2 \). Let two corresponding secret pixels in the first and second secret images are \{100, 200\} and \{50, 150\}, respectively, in a component. Let the corresponding blocks in shares 1 and 2 generated after Step 2 in encryption are \{0, 255, 255, 0\} and \{0,
255, 0, 255), respectively, which correspond to share block generation for white pixels in both cover images and white pixel in authentication image, where 0 is the black pixel and 255 is the white pixel in the RGB colour model. Using Equation (1), secret pixels of secret image 1 and secret image 2 are converted into cipher values \{172, 239\} and \{164, 5\}, respectively; 172 = (10 \times 16) + 12, 239 = (14 \times 16) + 15, 164 = (10 \times 16) + 4 and 5 = (0 \times 16) + 5. Values 172 and 164 are stored in the block of share 1, and values 239 and 5 are stored in the block of share 2. After encryption, modified block contents in shares 1 and 2 are \{10, 252, 244, 10\} and \{14, 255, 0, 245\}, respectively. During decryption, original cipher values are obtained after Step 4 as \{172, 164\} from share 1’s block and \{239, 5\} from share 2’s block. Applying Equation (2) on \{172, 239\} and \{164, 5\}, we get back the original secret pixels \{100, 200\} and \{50, 150\}, respectively.

4 | PROPERTIES ANALYSIS

In this section, the \((v, z)\)–LAMSIS scheme is proven to be a valid one by Theorems 1–3, having properties such as security, contrast and cheating prevention. We have also analysed about the size of shares, cover images and authentication image for general values of \(v\) and \(z\), and about the quality of shares.

4.1 | Security and contrast properties

Theorems 1 and 2 are used to prove the security and contrast properties of the \((v, z)\)–LAMSIS scheme, respectively.

**Theorem 1** The \((v, z)\)–LAMSIS scheme is secure.

*Proof:* The original \(z\) shares are generated by using \((v, z)\)–EVCS which is already proven to be secure and each block of \(m\) pixels is embedded with cipher values of \(m/2\) secret images computed using \((v, z)\)–PISSS which is also already proven to be secure. Secure means less than \(v\) shares cannot disclose information about the secret image. Hence, the \((v, z)\)–LAMSIS scheme is as strong as \((v, z)\)–EVCS and \((v, z)\)–PISSS.

**Theorem 2** The secret images can be disclosed by using \(t\) (\(t \ge v\)) shares in the \((v, z)\)–LAMSIS scheme.

*Proof:* As the cipher values generated using \((v, z)\)–PISSS with respect to each secret image are stored in shares generated using \((v, z)\)–EVCS, a minimum of \(v\) in \(t\) shares are sufficient to recover the secret image pixels and, hence, recover all the secret images.

4.2 | Cheating prevention

Authentication for cheating prevention in the \((v, z)\)–LAMSIS scheme is implemented using the stacking operation carried out by the dealer. A successful cheating devolves on the correct supposition of the authentication image pixels by stacking the shares of victim(s) and cheater(s), and finding all pixel values of secret images correctly. We consider two types of cheaters: malicious participant (MP) and malicious outsider (MO) as discussed in [3]. MP is a cheater who is a licit participant and MO is a cheater who is not in the set of licit participants.

**Theorem 3** The \((v, z)\)–LAMSIS scheme is cheat immune to \(t'\), \(1 \le t' \le z-1\) cheaters.

*Proof:* According to distinct number \(t'\) and kinds of cheaters, the proof for cheat immunity of the proposed scheme is explained with respect to four cases as follows: (i) an MO has no details about the shares of the licit participants. The only thing he can carry out is make some fake shares which can reveal fake secret images using Equation (2) and give it to a dealer for decryption. But, cheating will be noticed in Step 1 of decryption. (ii) An MP has only information about his share and cover image. The only thing he can do is to create some extra fake shares for revealing fake secret images of his choice and deliver it to a dealer for decryption. But again, cheating will be noticed in Step 1 of decryption. (iii) For \(t' < \sqrt{v}\) MP, they do not get information about authentication image as authentication image is shared using \((v, z)\)–EVCS. So, they also fail during authentication in Step 1 of decryption. (iv) For \(\sqrt{v} \le t' \le n-1\) MP, they have information about authentication image obtained by stacking their shares. They create fake shares in such a way that on stacking them with victim’s share, authentication image is obtained. But, as they do not have information about victim’s share, they cannot recover the secret images using Equation (2) that they wanted to show to the victim after decryption. This is because the cipher values embedded in the victim’s share generated using Equation (1) are unique for original secrets. When these cipher values are used with the ciphers values of fake shares in Equation (2), wrong secret pixel values are generated, failing to cheat the victim.

4.3 | Size of shares, cover images and authentication image

To share secret images, each of size \(f \times g\) using \((v, z)\)–LAMSIS scheme, cover images and authentication image, each of size \(f \times (g/v)\) are used, where \(f\) is the height and \(g\) is the width of a secret image. If \(m\) is the pixel expansion of the scheme, then the size of each share becomes \(f \times ((g/v) \times m)\). Using these facts, we will prove that the overall size of shares produced using the proposed scheme is lesser than or equal to the overall size of shares produced using any general \((v, z)\)–VCS with pixel expansion 1 for sharing \(r\) secret images, each.
of size \( f \times g \), is less than or equal to the total size of shares generated using any general \((v, z)\)–VCS with pixel expansion 1 sharing one secret image at a time.

**Proof:** For the proposed scheme, we know that the size of each share is \( f \times ((g/v) \times m) \) which carries information about \( r = m/2 \) (i.e. \( m = 2r \)) secret images. Therefore, the total size of shares \( TS_{(v, z)}\)–LAMSIS is \( z \times f \times ((g/v) \times 2r) \). For general \((v, z)\)–VCS with pixel expansion 1, the size of each share is \( f \times g \). Therefore, the total size of shares \( TS_{general} \) is \( z \times f \times g \times r \) for sharing \( r \) secret images. Without loss of generality, as \( v \geq 2, z \times f \times (g/v) \times 2r \leq z \times f \times g \times r \), that is, \( TS_{(v, z)}\)–LAMSIS \( \leq TS_{general} \). To be exact, for \( v = 2, TS_{(v, z)}\)–LAMSIS = \( TS_{general} (v, z) \) and for \( v > 2, TS_{(v, z)}\)–LAMSIS \( < TS_{general} (v, z) \).

For example, in \((2, 3)\)–LAMSIS scheme, \( m = 6 \). It means the number of secret images \( r \) that can be shared is \( m/2 = 6/2 = 3 \). Let the size of each secret image be \( 100 \times 90 \). Then, the size of each cover image and authentication image is \( 100 \times (90/2) \). From the proof of Lemma 1, \( TS_{(2, 3)}\)–LAMSIS = \( 3 \times 100 \times (90/2) \times 6 = 81,000 \) and \( TS_{general} (2, 3) = 3 \times 100 \times 90 \times 3 = 81,000 \), that is, \( TS_{(2, 3)}\)–LAMSIS \( = TS_{general} (2, 3) \). Similarly, in \((3, 3)\)–LAMSIS scheme, \( m = 6 \). So, \( r = 3 \). By keeping the size of each secret image as the same as before, the size of each cover image and authentication image is \( 100 \times (90/3) \). Now, \( TS_{(3, 3)}\)–LAMSIS = \( 3 \times 100 \times (90/3) \times 6 = 54,000 \) and \( TS_{general} (3, 3) = 3 \times 100 \times 90 \times 3 = 81,000 \) that is \( TS_{(3, 3)} < TS_{general} (3, 3) \).

### 4.4 Quality of shares

Visual quality of shares is assessed using **peak-signal-to-noise ratio** (PSNR). The higher the PSNR value, the higher the quality is. PSNR of the revealed image in respect of the original image is given by

\[
\text{PSNR} = 10 \log_{10} \left( \frac{255^2}{\text{MSE}} \right) \tag{3}
\]

where MSE is the mean square error computed by

\[
\text{MSE} = \frac{1}{f \times g} \sum_{i=1}^{f} \sum_{j=1}^{g} (x_{ij} - y_{ij})^2 \tag{4}
\]

In Equation (4), \( f \) is the height and \( g \) is the width of the image, \( x_{ij} \) and \( y_{ij} \) are the original pixel value and transformed pixel value at the same position, respectively. We give the lowest bound on the PSNR value of a share generated using the proposed scheme after embedding the cipher values that is at the end of encryption, with respect to the corresponding share before embedding cipher values that is, after Step 2 of encryption, in Lemma 2.

**Lemma 2** The minimum PSNR value of a share generated using the proposed \((v, z)\)–LAMSIS scheme is 24.608 dB with respect to the corresponding share before embedding the cipher values.

**Proof:** The maximum difference that can be obtained between original and transformed pixel values at a position is 15. If this maximum difference is considered to be the same for all pixel positions, then this will be the scenario where the PSNR value will be at its least. For this condition, Equation (4) becomes

\[
\text{MSE} = \frac{1}{f \times g} \sum_{i=1}^{f} \sum_{j=1}^{g} 15^2,
\]

\[
\text{MSE} = 15^2.
\]

Now, by substituting this MSE value in Equation (3), we get

\[
\text{PSNR} = 10 \log_{10} \left( \frac{255^2}{15^2} \right)
\]

\[
\text{PSNR} = 20 \log_{10} \left( \frac{255}{15} \right)
\]

\[
\text{PSNR} = 20 \times 1.2304
\]

\[
\text{PSNR} = 24.608 \text{ dB}
\]

From Lemma 2, it is clear that even after embedding cipher values into intermediate shares, the finally generated shares would not lose their visual meaning.

### 5 RESULTS AND COMPARISON

#### 5.1 Experimental results

The experimental results for the \((2, 2)\)–LAMSIS and \((2, 3)\)–LAMSIS are depicted in Figures 4 and 5, respectively, to show that the scheme proposed can be applied for both \((v, v)\) and \((v, z)\).

In Figure 4, *Puffin* and *Tiger* images are used as secret images, each having size \( 256 \times 256 \). *Lena* and *Scilab* images are used as cover images, each of size \( 256 \times 128 \). *Nitte logo* image is used as an authentication image of size \( 256 \times 128 \). Produced shares are of size \( 256 \times 512 \). The pixel expansion is 4, which means that the number of secret images shared is \( 4/2 = 2 \). Figure 4c shows the intelligible shares which can be visually recognised as *Lena* and *Scilab* images. Figure 4d shows the stacked result of shares 1 and 2, which displays the authentication image indicating that there is no cheating done. On successful authentication, secret images are recovered without loss of information as the same as in Figure 4a. Here, the total size of shares is \( 2 \times 256 \times 512 = 262,144 \), which is equal to \( 2 \times 256 \times 256 \times 2 = 262,144 \), which is the total size of shares generated for sharing two secrets of size \( 256 \times 256 \) using \((2, 2)\)–VCS having pixel expansion 1 as proved in Lemma 1.
\textbf{FIGURE 4} (2, 2)–LAMSIS scheme: (a) first and second secret images (from left to right), (b) first and second cover images and authentication image (from left to right), (c) share 1 and share 2 (from left to right), and (d) share 1 + share 2.

\textbf{FIGURE 5} (2, 3)–LAMSIS scheme: (a) first, second and third secret images (from left to right); (b) first, second and third cover images (from left to right); (c) shares 1, 2 and 3 (from left to right); (d) share 1 + share 2, share 1 + share 3, share 2 + share 3 and share 1 + share 2 + share 3 (from left to right).

In Figure 5, Airplane, Bike and People images are used as secrets with a size of 256 $\times$ 256 each. Baboon, Balloons and Peppers images are used as cover images with a size of 256 $\times$ 128 each. Here, Nitte logo image is used as an authentication image of size 256 $\times$ 128 as the same as in Figure 4b.

The size of each intelligible share depicted in Figure 5c is 256 $\times$ 768. The pixel expansion is 6 and the number of secrets shared is 6/2 = 3. Figure 5d depicts the stacked result of various combinations of shares revealing the authentication image after which decryption is done to recover the secret images by using any combination of minimum two distinct shares, as the same as in Figure 5a. Here, the total size of shares is 3 $\times$ 256 $\times$ 768 = 589,824, which is equal to 3 $\times$ 256 $\times$ 256 $\times$ 3 = 589,824, which is the total size of shares generated for three secrets of size 256 $\times$ 256 using (2, 3)–VCS with pixel expansion 1.

PSNR is calculated for reconstructed secret images, reconstructed authentication image and shares as in Figures 4 and 5 with respect to their corresponding original images and they are displayed in Tables 1 and 2. It can be noted from Tables 1 and 2 that all the PSNR values of shares and reconstructed authentication images obtained from different combination of shares' stacking are small indicating low quality. The PSNR values of all revealed secret images are infinite which implies that the reconstruction is lossless.

In Figure 6, we have shown the results of cheating in (2, 3)–LAMSIS scheme with two MPs for the example taken in Figure 5. Participants 1 and 2 are MPs trying to cheat
participant 3 who has a valid share, with fake secret images depicted in Figure 6a which are Emblem, Kalam and Rajkumar images having a size of 256 × 256 each, respectively. The fake share 1 and fake share 2 created by participants 1 and 2, respectively, have the same meaning as shares 1 and 2 as in Figure 5c. As discussed in case 4 of proof of Theorem 3, the fake shares are created by participants 1 and 2 in such way that, on stacking them with each other and with valid share of participant 3, an authentication image is obtained as shown in Figure 6b. Using fake share 1 and fake share 2, fake secret images are reconstructed as the same as in Figure 6a. When fake share 1 and valid share are used to reconstruct the fake secret images, distorted images as shown in Figure 6c are obtained. Similarly, distorted images as shown in Figure 6d are obtained when fake share 2 and valid share are used to reconstruct the fake secret images. It can be seen that cheaters fail to cheat the victim with fake secret images as proved in Theorem 3.

5.2 | Comparison

The scheme proposed is compared with schemes in [6–21] with respect to properties such as intelligible shares, authentication for cheating prevention, number of secret images shared, restriction on v and z, and lossless recovery of secret images as shown in Table 3. A number of secret images shared, for schemes in [12,14,18], are written as ‘Multiple’. It means that the count of secret images shared can be any number greater than 1 which is decided by the participants involved.

TABLE 1  PSNR values of images in Figure 4

| Image               | PSNR (dB) |
|---------------------|-----------|
| Share 1             | 5.9248    |
| Share 2             | 6.0760    |
| Share 1 + Share 2   | 2.2230    |
| Revealed first secret image | Infinite |
| Revealed second secret image | Infinite |

Abbreviation: PSNR, peak-signal-to-noise ratio.

TABLE 2  PSNR values of images in Figure 5

| Image               | PSNR (dB) |
|---------------------|-----------|
| Share 1             | 5.9186    |
| Share 2             | 6.6471    |
| Share 3             | 6.3093    |
| Share 1 + Share 2   | 1.8072    |
| Share 1 + Share 3   | 1.8141    |
| Share 2 + Share 3   | 1.8558    |
| Share 1 + Share 2 + Share 3 | 1.7847 |
| Revealed first secret image | Infinite |
| Revealed second secret image | Infinite |
| Revealed third secret image | Infinite |

Abbreviation: PSNR, peak-signal-to-noise ratio.

FIGURE 6  Cheating in (2, 3)–LAMSIS scheme with 2 MPs: (a) first, second and third fake secret images (from left to right); (b) fake share 1 + fake share 2, fake share 1 + valid share and fake share 2 + valid share (from left to right); (c) revealed first, second and third secret images from fake share 1 and valid share (from left to right); (d) revealed first, second and third secret images from fake share 2 and valid share (from left to right), where valid share is share 3 in Figure 5c.
Using the scheme proposed, a maximum of $m/2$ secret images can be dealt at once and the recovery of all secret images is perfect without any loss. From the comparison details in Table 3, it is seen that the scheme in [12] has whip hand over the proposed scheme in respect of the number of secret images shared, and the proposed scheme has whip hand over scheme in [12] in respect of lossless recovery of secret images. Other known limitations of scheme in [12] which are not present in the proposed scheme are as follows: (i) extra burden of carrying information about number of PISS pixels and authentication bits in shares; (ii) a constraint on the size of the secret images that PISS shadows have to be created with respect to threshold $v$ and radius of circular shares; (iii) difficult to find the reference points of rotation for shares; (iv) shares have to be circumvolved in a specific way to reconstruct each of the multiple secret images. So, the proposed scheme has more advantages over the compared schemes.

### 6 CONCLUSION AND FUTURE WORK

Theoretically and experimentally, we proved that the $(v, z)$–LAMSIS scheme is a valid multiple secret images' sharing scheme with resistance to cheating and with perfect reconstruction of secret images, using polynomials and extended visual cryptography. It has been also shown that the overall size of shares created by using this scheme is either less than or equal to the overall size of shares created by any general $(v, z)$–VCS having pixel expansion 1 sharing one secret image at a time, which makes the $(v, z)$–LAMSIS scheme optimal in respect of storage space and bandwidth utilisation comparatively. From the comparison analysis, it has been inferred that the proposed scheme has more applications.

It has been noticed that the visual quality of intelligible shares and reconstructed authentication images are low when compared to that of their respective original images. It is also possible for a minimum $v$ number of MPs to pass the authentication even though they fail to cheat the victim. Compared to multiple secret images sharing schemes in [15–17,19–21], which have no pixel expansion, the proposed scheme has higher pixel expansion. Therefore, the future scope of this research work is focussed on improvements in respect of low visual qualities, authentication abilities, number of secret images shared and pixel expansion.

### ORCID

Krishnaraj Bhat  |
https://orcid.org/0000-0003-2448-898X

### REFERENCES

1. Naor, M., Shamir, A.: Visual cryptography. In: De Santis, A. (ed.) Advances in Cryptology – EUROCRYPT'94: Lecture Notes in Computer Science, vol. 950, pp. 1–12 (1995)
2. Ateniese, G., et al.: Extended capabilities for visual cryptography. Theor. Comput. Sci. 250, 143–161 (2001)
3. Hu, C.-M., Tzeng, W.-G.: Cheating prevention in visual cryptography. IEEE Trans. Image Proc. 16(1), 36–45 (2007)
4. Ren, Y., et al.: Cheating prevention visual cryptography scheme with Latin square. IET Inf. Secur. 11(4), 211–219 (2017)
5. Ranjan Kumar, H.S., et al.: Cheat immune visual cryptography for secure transmission of images. Int. J. Eng. Adv. Technol. 8(4), 1175–1181 (2019)
6. Lin, S.-J., Lin, J.-C.: VGCSS: a two-in-one two-decoding-options image sharing method combining visual cryptography (VC) and polynomial-style sharing (PSS) approaches. Patt. Recogn. 40, 3652–3666 (2007)
7. Yang, C.-N., Ciou, C.-B.: Image secret sharing method with two-decoding-options: lossless recovery and previewing capability. Image Vis. Comput. 28, 1600–1610 (2010)
8. Peng, L., et al.: Improvements of a two-in-one image secret sharing scheme based on gray mixing model. J. Vis. Commun. Image R. 57, 39–47 (2018). https://doi.org/10.1016/j.jvcir.2018.10.014
9. Kapadiya, V.J., Desai, L.S., Meghrajani, Y.K.: Boolean-based multi secret image sharing scheme based on Boolean operations. J. Vis. Commun. Image R. 57, 39–47 (2018). https://doi.org/10.1016/j.jvcir.2018.10.014
10. Deshmu kh, M., Nain, N., Ahmed, M.: A novel approach for sharing multiple color images by employing Chinese Remainder Theorem. J. Vis. Commun. Image R. 57, 39–47 (2018). https://doi.org/10.1016/j.jvcir.2018.10.014
11. Prasetyo, H., Guo, J.-M.: A note on multiple secret sharing using Chinese remainder theorem and exclusive-OR. IEEE Access. 7, 37473–37497 (2019)
12. Shamir, A.: How to share a secret. Commun. ACM. 22(11), 612–613 (1979)
13. Thien, C.-C., Lin, J.-C.: Secret image sharing. Comput. Graph. 26, 765–770 (2002)
14. Zhou, X., et al.: Lossless and efficient polynomial-based secret image sharing with reduced shadow size. Symmetry. 10(7), 1-16 (2018). https://doi.org/10.3390/sym10070249

How to cite this article: Bhat K, Reddy K.R. UK, Kumar H.S. R, Mahto D. A novel scheme for lossless authenticated multiple secret images sharing using polynomials and extended visual cryptography. *IET Inf. Secur*. 2021;15:13–22. [https://doi.org/10.1049/ise2.12001](https://doi.org/10.1049/ise2.12001)