A Fast and Hardware-Efficient Visual Cryptography Scheme for Images

Dipesh Vaya and Sarika Khandelwal

Abstract Shamir's encryption method is to share a secret image by n number of shadow images and then r shadow images can be used to obtain the original secret image. In proposed method, the size of secret image is greater than the size of the shadow image used for the encryption. Such shadow image is beneficial to process in image hiding, transmission, or storage. For this purpose Shamir's encryption technique is used in this proposed work. In Shamir's encryption technique, author used the equation to encrypt the data into multiple parts. In the equation, time required for the multiplication and division of the input components of the data is more than addition and subtraction. Hence, the encryption time is little bit high. To reduce this encryption and decryption time, Shamir's equation is modified by converting all the multiplication part into addition and division parts into subtraction in this proposed work.

Keywords Secret sharing · Lossless reveal · Shadow images · Shamir's encryption technique

1 Introduction

Secret images and texts often exist in the military or commercial application. About the storage of the secret images or data, the security is one of the most important concerns. In last few years, different methods were proposed by different researchers to improve the security of data or images; examples include image hiding and watermarking. But one of the major drawback of these methods are, the

D. Vaya (✉) · S. Khandelwal
Department of Computer Science & Engineering, Geetanjali Institute of Technical Studies, Udaipur, India
e-mail: dipesh.vaya88@gmail.com

S. Khandelwal
e-mail: sarikakhandelwal@gmail.com

© Springer India 2016

S.C. Satapathy et al. (eds.), *Proceedings of the Second International Conference on Computer and Communication Technologies*, Advances in Intelligent Systems and Computing 379, DOI 10.1007/978-81-322-2517-1_14

secret data is transfer through single information carrier and if this carrier is lost or crippled during transmission, the secret data cannot be revealed completely. In order to overcome this problem, multiple duplicates of the information carrier can be used, but because of this the security danger of exposure will also increase. Secret sharing method can be used to solve this problem.

Blakley [1] and Shamir [2] proposed the concept of secret sharing independently. This proposed method was known as the (k; n) threshold scheme. In most of the studies, main focus is on the security of the secret key of the encryption data [3–5]. Number of bytes used in the digital image are generally very large and the gray value of the digital image is bounded (0–255). Hence when the image is used as the secret data in the threshold scheme directly, this will waste memory space and more time required for encryption of image and obtaining original image from the shadow image. Therefore, need of the specific method for secret image sharing is obtained. A new secret image sharing method derived using the (k; n) threshold scheme proposed by Shamir is proposed in this paper. The time required to convert the shadow images is much less than that of the secret image in our method. We will require that

- The n shadow images are generated using secret image.
- To reconstruct the image any k or more than k shadow images can be used.
- Any $k - 1$ or less shadow images cannot get sufficient information to reveal the secret image, i.e., secret image cannot be obtain from any $k - 1$ or less shadow images.

2 Shamir's (k, n) Threshold Scheme

This paper roughly introduces his scheme first, because proposed method is based on the (k, n) threshold scheme proposed by Shamir. If the secret data D is divided into n shadows, i.e., $(D_1, D_2, \ldots D_n)$, and we want original secret data cannot be retrieve from the encrypted data without k or more shadows. Without loss of generality, let us take any number as the D. Pick randomly a prime number p and a $k - 1$ degree polynomial to split D into n shadows [1, 6].

$$q(x) = (a_0 + a_1 x + \cdots + a_{k-1} x_{k-1}) \bmod p, \tag{1}$$

In which $a_0 = D$ and then evaluate

$$D_1 = q(1), \ldots D_i = q(i), \ldots, D_n = q(n) \tag{2}$$

Note that each D_i is a shadow. The coefficients $a_1, \ldots, a_{k-1}$ in $q(x)$ are randomly chosen from the integers in $0 - (p - 1)$. Given any k pairs of these n pairs $\{i, D_i\}_i^n = 1$ we can find the coefficients $a_0 - a_{k-1}$ of $q(x)$ by the Lagrange's

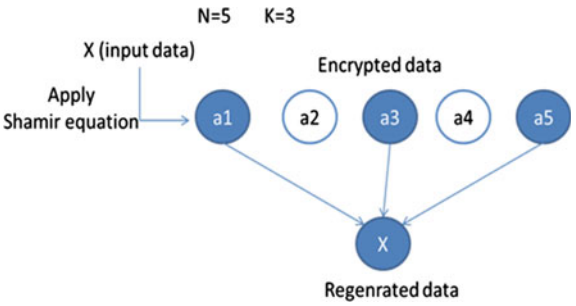

Fig. 1 Scenario of Shamir threshold equation

interpolation, and hence the secret data $D = a_0$ is also revealed. Figure 1 shows the overall functionality of the Shamir threshold equation where n is number of encryption parts and k is number of reconstruction parts.

In image sharing, to use Shamir's (k, n) threshold scheme directly, the gray value of the first pixel is taken as a_0, then we obtain the corresponding output $q(1) - q(n)$; Once the output is obtained then the value of a_0 is replaced by second pixel's gray value, and this process is repeated until all the pixels of secret image are processed.

If we want to divide D secret image into n number of shadow images, i.e., $(D_1, \ldots, D_n)$, and r or more shadow images are used to reveal the secret image from the information carrier. We generate the $r - 1$ degree polynomial, by letting the r coefficients, will be the gray values of r pixels in our proposed method. We use no random coefficient in proposed method where in Shamir's method he uses random coefficient, this is the main difference between our and Shamir's method. The gray value of the image pixel is between the 0 and 255, because of this Shamir let the prime number p be 251 which is the greatest prime number not larger than 255. We must truncate all the gray value to 250 from 251 to 255 of the secret image so that all the gray values are in the range of 0–250.

First the image is divided into several sections for the encryption process. Every section of the secret image has k number of pixels, and every pixel of the image belongs to one and only one section of the secret image. For every section of j define the following $k - 1$ degree polynomial

$$q(j) = (a_0 + a_1 x + \cdots + a_{k-1} x_{k-1}) \text{mod} 251, \tag{3}$$

where $a_0, \ldots, a_{k-1}$ are the k pixels of the section, and then evaluate

$$q_j(1), q_j(2), \ldots, q_j(n). \tag{4}$$

Output obtained from the equations is the n output pixels $q_j(1) - q_j(n)$ of the j section are assigned sequentially to the n shadow images. Every shadow image receives one generated pixel of the secret image for each section (of k pixel). Secret image sharing method proposed here follows the following steps:

- Reduce all the gray values of the secret image larger than 250 to in the range of 0–250.
- To generate a permutation sequence to permute the pixels of the secret image use a secret key.
- To form a section take k not-shared-yet pixel of the permuted image sequentially.
- To generate n pixels for the n shadow images, use the section formed in Step 3 and Eqs. (3) and (4).
- Until all pixels of the permuted Images are processed repeat Steps 3 and 4 constantly.

The reveal phase using any k shadow images are as follows:

- From every k shadow images take the first non-used pixel.
- Improvise every k pixels and apply the Lagrange's interpolation to solve for the coefficients $a_0 - a_{k-1}$ in Eq. (3). The coefficients $a_0 - a_{k-1}$ are then the corresponding k pixel values of the permuted image.
- Until all pixels of the k shadow images are processed repeat Steps 1 and 2.
- To get the secret image, apply inverse permutation operation to the permuted image.

Figure 2 shows the experimental results of the Shamir's secret sharing encryption technique taken from paper presented by Thien and Line [7].

The value of $n = 4$ used in the encryption technique and value of $k = 2$. So after encryption of the original image using Shamir's secret sharing encryption technique four shadow images are generated and to obtain the original image from the encrypted shadow image, two shadow images are combined because value of $k = 2$ is used in the Shamir's encryption equation.

3 Related Work

El-Tigani et al. [8] introduced a new (x, n) threshold secret sharing method for grayscale images. Here quadratic residues method is incorporated to encrypt the image and after that Shamir's methodology is used to create the shadow images. The major concern of author is to allow any number of participants for sharing secret image in any communication channel. As compared to Chen-Chang's technique [9], this work provides more flexibility and security for image sharing.

Patil et al [10] proposed a method of encryption to construct colored EVC scheme to improve visual image quality with error diffusion and VIP synchronization. For retaining the original values of pixel, the pixels positions are synchronized that contain visual information of original images over the color channels.

Kalai Selvi et al [11] proposed new algorithm to generate a random polynomial of the secret image for the sharing purpose. This proposed process offers enhanced technique of encryption. In this algorithm, the image is encrypted after several

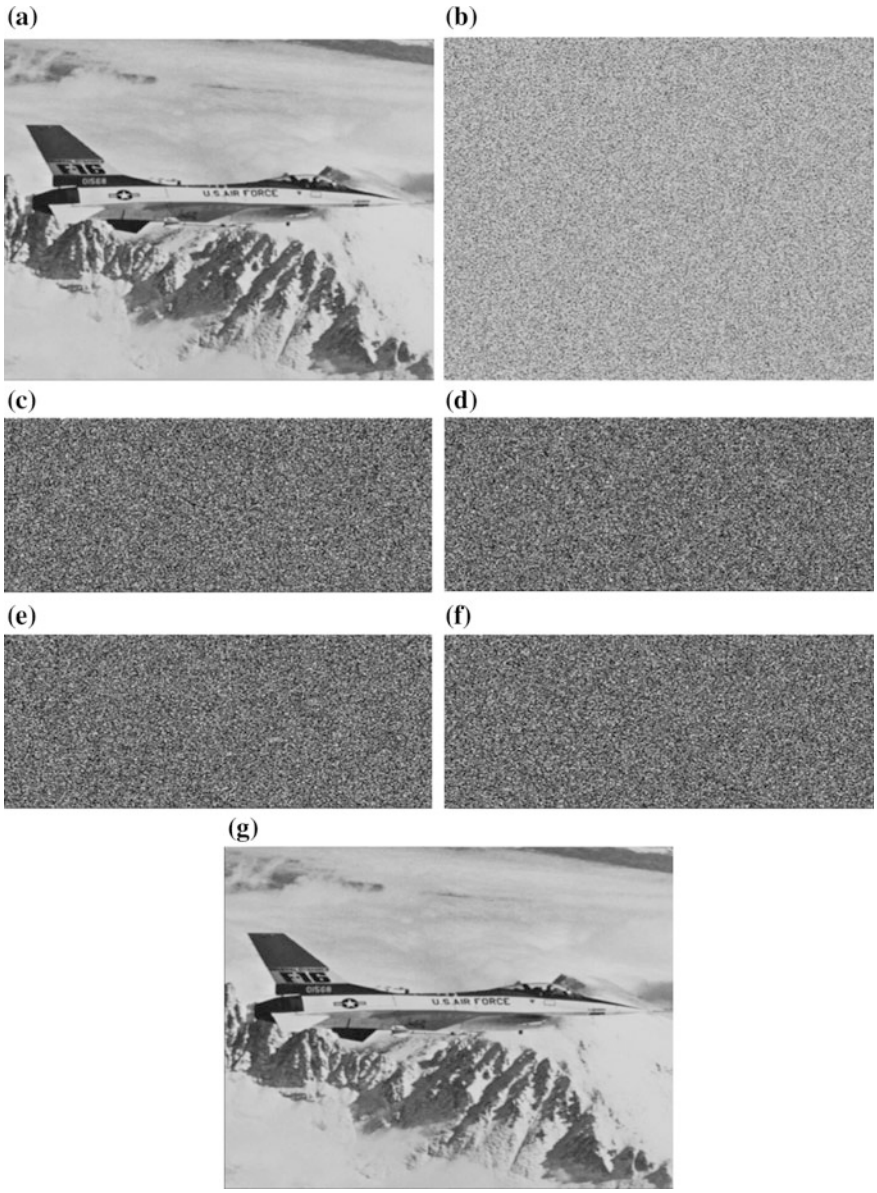

Fig. 2 **a** A 512 × 512 secret image; **b** the permuted image of (**a**); **c**–**f** the four shadow images; **g** the revealed image

numbers of rounds, which makes the computation more complex. As Compared to the encryption schemes based on the secret sharing, image size is far bigger than the secret share's size.

4 Proposed Methodology

The proposed work aims to reduce the time required for encryption and regeneration of image so that the process of sharing and regeneration is fast. For image sharing, Shamir's secret sharing encryption technique is applied with enhanced features.

This paper proposes a method for enhancement of Shamir's secret sharing encryption algorithm where we convert all higher level mathematical operation of Shamir's encryption to lower level operations i.e., this work enhances Shamir's work by implementing all multiplication operations into addition and all division operations by subtraction.

In Shamir's encryption equation, array multiplier is used for encrypting the image. A carry save array multiplier is also known as a simple parallel array multiplier. But it can be used to perform only over signed bits due to restrictions. To remove the logic registers from the array multiplier, array of AND gates are used in the structure and adders in iteratively arranged manner [12]. In original Shamir encryption algorithm, image pixels are stored inside array and then multiplication is applied on the different arrays to give the output array.

$$\text{Data 1} = \text{array of pixels}$$
$$\text{Data 2} = \text{array of pixels}$$
$$\text{Data 1} \times \text{Data 2} = \text{Output Array}$$

More processes are required to implement the multiplication array, because more adders are required to execute the multiplication and it requires more time and energy to process the encryption. For any array multiplier area, computation speed and dissipation of power are the important criteria. To improve these parameters, array adders are used in the proposed method. Parallel prefix adder can perform operations in higher speed. It is most flexible and commonly used adder for binary addition. For optimizing the fan out, area, inter connection count, and logic complexity, different researchers have been proposed number of architectures for designing parallel prefix adder. Lots of works so far have been done in past and considerably various architectures have been proposed for designing an adder. When operations required to be occur on high speed, parallel prefix adders are required to be in tree like structure [13]. To implement array adders in the Shamir's encryption equation, higher order operations are converted to the lower order operations. The original Shamir's encryption equation is

$$x^{(1:k-1)*r} + s \tag{5}$$

By converting the higher operation in the equation by lower operation, we obtained the equation as

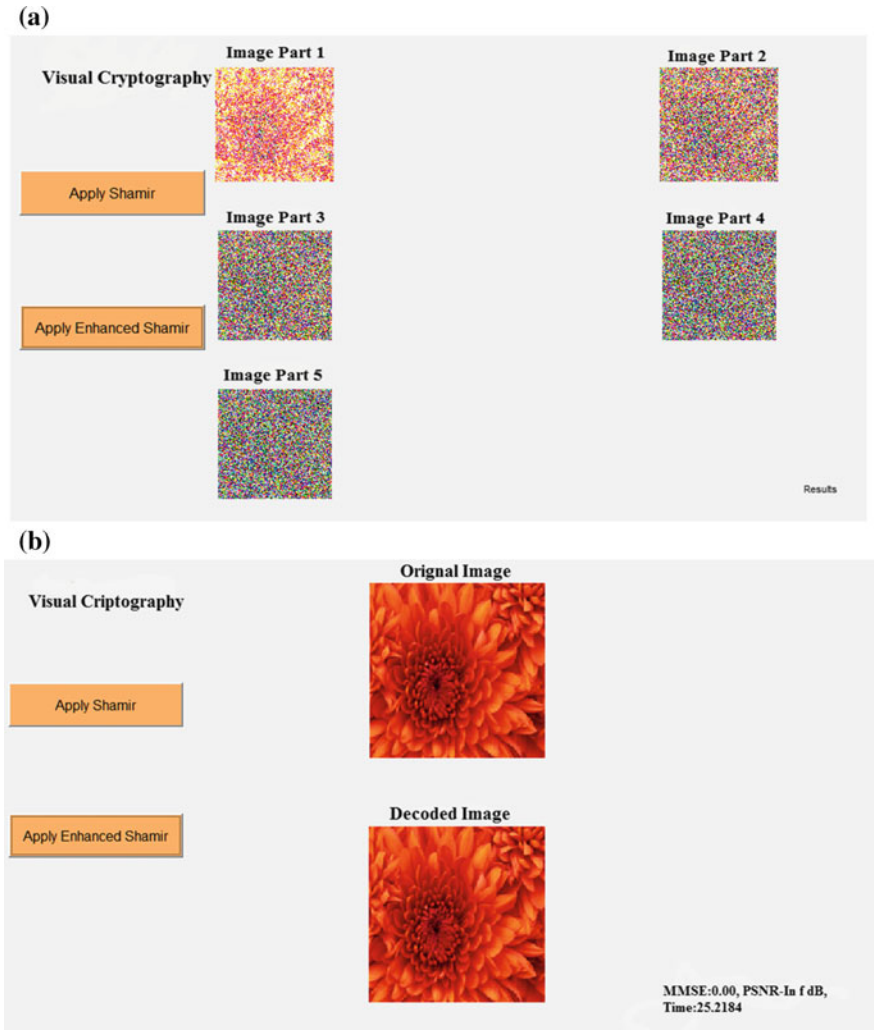

Fig. 3 **a** Output after applying proposed encryption technique; **b** output after applying proposed decryption technique on an image

$$x^{\sum_{i=1}^{r}(1:k-1)} + s \tag{6}$$

5 Experimental Result

MATLAB software is used to implement the proposed encryption technique on images. The experimental results are shown below:

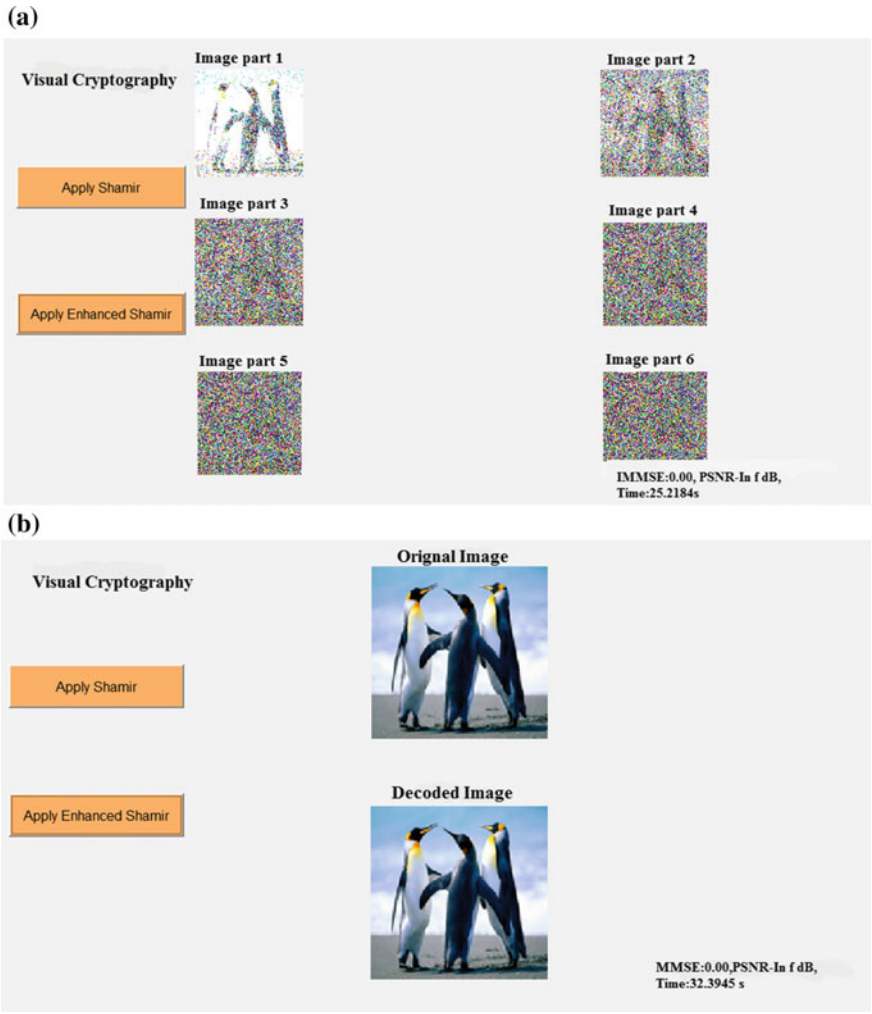

Fig. 4 **a** Output after applying proposed encryption technique; **b** output after applying proposed decryption technique on an another image

Figures 3a, b and 4a, b show the experimental results of proposed encryption and decryption techniques output on images of flower and penguins respectively.

Table 1 shows the comparison of time required to encrypt and decrypt the image using proposed technique and Shamir's technique and Fig. 5 shows the graphical representation of the comparison.

Table 1 Result of proposed and simple Shamir's techniques

Image size	Time (s) (Shamir)	Time (s) (Enhanced Shamir)
128 × 128	47.25	25.3
256 × 256	75.36	38.45
512 × 512	102.97	47.44
1024 × 1024	165.89	74.56

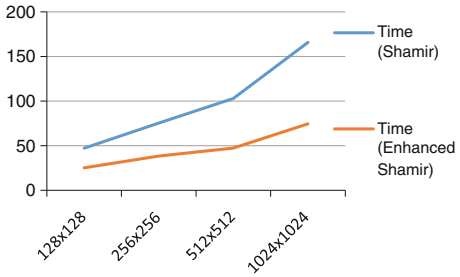

Fig. 5 Graphical representation of the comparison between Shamir and Enhanced Shamir algorithms

6 Conclusion

The proposed method works effectively and efficiently over time optimization for the image transmission. In this paper, we improved the Shamir's encryption and decryption equation for the better utilization of the time. As shown in the Table 1, we are able to reduce the time of encryption and decryption of the image by 45–60 %. For reducing the time, we have converted all the multiplication into addition and all the division into subtraction in the original Shamir's equation to obtain enhanced Shamir's equation. In this paper, Shamir's encryption technique is used for the encryption; in future any other advance encryption technique can be used to improve the efficiency of the proposed system.

References

1. Blakley, G.R.: Safeguarding cryptographic keys. In: Proceedings AFIPS 1979 National Computer Conference, vol. 48, pp. 313–7. New York, USA, 4–7 June 1979
2. Shamir, A.: How to share a secret. Commun. ACM **22**(11), 612–613 (1979)
3. Ahlswede, R., Csiszár, I.: Common randomness in information theory and cryptography-part I: secret sharing. IEEE Trans. Inf. Theory **39**(4), 1121–32 (1993)
4. Beimel, A., Chor, B.: Secret sharing with public reconstruction. IEEE Trans. Inf. Theory **44** (5), 1887–1896 (1998)

5. Beimel, A., Chor, B.: Universally ideal secret-sharing schemes. IEEE Trans. Inf. Theory **40**(3), 786–794 (1994)
6. Stinson, D.R.: Decomposition constructions for secret-sharing schemes. IEEE Trans. Inf. Theory **40**(1), 118–124 (1994)
7. Thien, C.-C., Jin, J.-C.: Secret image sharing. Comput. Graph. **26**, 765–770 (2002)
8. Abdelsatir, E.-T.B., Salahaldeen, S., Omar, H., Hashim, A.: A novel (K, N) secret sharing scheme from quadratic residues for grayscale images" Int. J. Netw. Secur. Appl. (IJNSA) **6**(4), 65–72 (2014)
9. Chen, C.-C., Chang, C.-C.: Secret image sharing using quadratic residues. Intell. Inf. Hiding Multimedia Sig. Process. (IIHMSP) **1**, 515–518 (2007)
10. Patil, S., Rao, J.: Extended visual cryptography for color shares using random number generators. Int. J. Adv. Res. Comput. Commun. Eng. **1**(6) (2012)
11. Kalai Selvi, A., Mohamed Sathik, M.: Secret sharing scheme for image encryption based on primitive root theorem. Int. J. Control Autom **5**(3), 37 (2012)
12. Thakur, M., Ashraf, J.: Design of braun multiplier with Kogge Stone Adder & it's implementation on FPGA. Int. J. Sci. Eng. Res. **3**(10) (2012)
13. Seng, Y.K. Roy, K.: Low Voltage, Low Power VLSI Subsystems. TMC (2009)