Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 89 (2016) 677 – 683

Procedia Computer Science

Twelfth International Multi-Conference on Information Processing-2016 (IMCIP-2016)

Secure $(n, n + 1)$-Multi Secret Image Sharing Scheme using Additive Modulo

Mohit Rajput and Maroti Deshmukh*

National Institute of Technology, Uttarakhand 246 174, India

Abstract

Multi Secret Image Sharing (MSIS) scheme is a protected method to transmit more than one secret images over a communication channel. Conventionally, only single secret image is shared over a channel at a time. But as technology grew up, there arises a need for sharing more than one secret image. An (n, n)-MSIS scheme is used to encrypt n secret images into n meaningless noisy images that are stored over different servers. To recover n secret images all n noise images are required. At earlier time, the main problem with secret sharing schemes was that one can partially figure out secret images by getting access of $n - 1$ or fewer noisy images. Due to this, there arises a need of secure MSIS scheme so that by using less than n noisy images no information can be retrieved. In this paper, we propose secure $(n, n + 1)$-MSIS scheme using additive modulo operation for grayscale and colored images. The experimental results show that the proposed scheme is highly secured and altering of noisy images will not reveal any partial information about secret images. The proposed $(n, n + 1)$-MSIS scheme outperforms the existing MSIS schemes in terms of security.

Peer-review under responsibility of organizing committee of the Organizing Committee of IMCIP-2016

Keywords: Additive Modulo; Correlation; Multi Secret Image Sharing (MSIS) Scheme; PSNR; RMSE.

1. Introduction

In present era, with enhancement of technology usage, digital media also increases swiftly. This increase concern over security in digital media. Due to this concern various techniques for data hiding were introduced. Some of them are Cryptography, Watermarking and Steganography. These methods are well known and highly used to hide the secret messages. Cryptography refers to process of converting plain text into encrypted form which is called as cipher text. In Cryptography we use keys to encrypt or decrypt data. Key refers to string of characters, which is used to decrypt or encrypt data at sender as well as receiver side. Main disadvantage associated with this method is sharing a key between sender and receiver. If some intruder gets access to the key, he can easily decode any secure message transfer between sender and receiver. Watermarking uses noise-tolerant signal and embeds it into digital media. The main disadvantage is, due to the introduction of noise-tolerant signal as it sometimes lead to error in decryption at receiver side. Steganography is an act to conceal secret data into other data.

Visual Cryptography, a secret sharing scheme first makes its entry when Adi[1] and Shamir[2] proposed a method, where a secret image is encrypted into noisy images which do not reveal any information about secret images.

*Corresponding author. Tel.: +91-8500173440.
E-mail address: marotideshmukh@nituk.ac.in

Peer-review under responsibility of organizing committee of the Organizing Committee of IMCIP-2016
doi:10.1016/j.procs.2016.06.034

Questions may arise, why do we need another secure method for security when we have enough of them? How secret sharing schemes have advantages over others? If somehow any intruder gets access to some noisy images it can't fabricate secret image from them which can be easily done in case of cryptography. On receiver side, it can be easily reconstructed without loss or with negligible loss. Secret sharing scheme has many application fields, including missile launch codes, areas where trust plays an essential role, sharing data over untrusted channels, highly classified information, access control etc. To achieve higher reliability and confidentiality, we use secret sharing scheme as by storing noisy images on different data servers increases reliability as well as confidentiality. Rest of the paper structure is as follows. Section 2, discuss the previous work made in the area of secret sharing schemes. The proposed $(n, n+1)$-MSIS schemes are presented in Section 3. In Section 4, the experimental results and analysis are shown. Section 5 concludes the paper and Finally, in Section 6 discusses future scope of MSIS schemes.

2. Related Work

Chen *et al.*[3] proposed $(n, n+1)$-MSIS scheme based on simple Boolean XOR operation. In this scheme, n secret images are used to create $n+1$ shared images and to decode them, all $n+1$ shared images are needed. In this scheme sharing capacity of multiple secret images are increased but it failed to produce randomized shared images because of simple Boolean XOR operation on secret images. Chen *et al.*[4] presented a secure Boolean based (n, n)-MSIS scheme. In this scheme to increase the randomness in shared images bit shift function is used. This scheme requires more time because of bit shift function. Lin *et al.*[10] proposed a novel random grid based MSIS scheme. Secret images are encoded into two pie shared images and it can be decoded by stacking one pie share on another at different angle of rotation. Daoshun *et al.*[6] proposed (n, n) scheme using XOR operation for gray scale images. In this (n, n)-MSIS scheme, n secret images are encrypted into n noisy images. No noisy image individually reveal any information about secret images but, if less than n images are stacked over each other, partial information is revealed. Shyong *et al.*[7] proposed a (n, n)-MSIS scheme using random grids for encryption of gray images as well as color images. Noisy images do not reveal any information when taken individually, whereas the secrets can be revealed when two noisy images are stacked over each other. Both of proposed method are accurate as no pixel expansion is seen. A (k, n)-RG based VSS scheme was proposed by Chen and Tsao[8] for binary and color images. A secret image is encrypted into n meaning less random grids. This scheme uses k shares to reveal secret image. Deshmukh *et al.*[9] presents a comparative study of (k, n) visual secret sharing scheme for binary images. Chen and Wu presented a secure scheme by using bit shift function. Bit shift is used to generate random image to provide the randomness in noisy images.

3. Proposed Method

With enhancement of technology, many MSIS scheme came into picture, some of them are $(n, n+1)$ and some are (n, n) *i.e.* they shares n secret images among n or $n+1$ receivers and to reconstruct these n secret images all n or $n+1$ noisy images are required. An $(n, n+1)$-MSIS scheme is an n-out-of-$(n+1)$ scheme. The main problem with many of the MSIS scheme was they reveal partial information from less than n or $n+1$ noisy images, which compromises security. Chen *et al.*[4] MSIS scheme reveal partial secret information from $(n-1)$ or fewer noisy images. Proposed scheme uses $n+1$ noisy shares to conceal n secret images and no partial information can be retrieved from n or less than $n+1$ noisy images. Proposed scheme uses additive modulo rather than XOR which is conventionally used. The main advantage of additive modulo over XOR operation is that it takes less time to execute. Boolean XOR operation has more time complexity than additive modulo as XOR perform bit by bit operation and XOR also reveals partial or complete information of secret image with less than n noisy images. As we move towards color image from binary image, number of bits increase from 1 to 24. We can easily figure out how rapidly time increases with increase in number of secret images and number of pixels in secret images. In additive modulo, there exists a unique additive inverse for every other element in the given range. Modular arithmetic are of two types; first is additive inverse and second is multiplicative inverse. In additive inverse, addition and modulo operations are used and in multiplicative inverse, multiplication and modulo operations are used. We say two numbers are additive inverse of each other if $a + b \equiv 0(mod\ n)$ where b and a are additive inverse of each other. Each integer has a unique additive inverse. For grayscale images and color images, pixel value ranges from $0 - 255$ and each number from $0 - 255$ has an additive inverse and its modulus value is 256, whereas each number may or may not have a multiplicative inverse in this range. We have used additive inverse rather than multiplicative inverse.

In this proposed scheme, n secret images SI_i, $i = 1, 2, \ldots, n$ are encrypted into $n + 1$ noisy images NI_i, $i = 1, 2, \ldots, n + 1$. Firstly, Temporary shares C_i, $i = 1, 2, \ldots, n$ are created by performing division operation on secret images $SI_i, i = 1, 2, \ldots, n$ with divisor as $n + 1$. To truncate floating points into respective closest integers we use round function, round function as it takes closest integer value and provide more precise results than ceil or floor function as shown in Table 1. Division operation is performed to reduce the pixel values. This is done so that, pixel values do not exceed from 255, when some scalar constant ($a \in N$) is multiplied with them. In second step, a random matrix R is created. In third step a server side key SK is generated by using additive modulo operation on $C_i, i = 1, 2, \ldots, n$. In final step, noisy images $NI_i, i = 1, 2, \ldots, n + 1$ are generated. n noisy images are generated by using additive modulo operation on temporary shares which is generated in step one C_i, $i = 1, 2, \ldots, n$, server side key SK and random matrix R *so*, Last noisy image NI_{n+1} is generated by using additive modulo operation on $n + 1$ times of server side key SK and $n+1$ times of random matrix. The main purpose of $(n+1)^{\text{th}}$ noisy image generation is to find random matrix R at receiver side. The noisy image generation algorithm of proposed $(n, n + 1)$-MSIS scheme is given in Algorithm 1.

The recovery procedure is different from encryption algorithm. This provides additional security as if, any intruder gets access to encryption algorithm then also he can't retrieve the secret information from noisy images. In recovery procedure we retrieve n secret images from $n + 1$ noisy images. In first step, generation of client side key CK is done by performing additive inverse operation on first n noisy images NI_i, $i = 1, 2, \ldots, n$. In second step we generate temporary noisy images P_i, $i = 1, 2, \ldots, n$ by performing multiplication on noisy images NI_i, $i = 1, 2, \ldots, n$ by $(n + 1)$ and using modular operation, here $(n + 1)$ is the number of noisy images send by sender. Third step deals with generation of random matrix R used at server end to provide randomness in pattern for noisy images. Random matrix R is generated by using additive inverse operation on $(n + 1)^{\text{th}}$ noisy image NI_{n+1} and client side key CK. Finally in fourth step, recovered images RI_i, $i = 1, 2, \ldots, n$ which is same as that of secret images. Recovered images RI_i, $i = 1, 2, \ldots, n$ are generated by using additive inverse operation on temporary noisy images P_i, $i = 1, 2, \ldots, n$, client side key CK and random matrix R. The recovery procedure of proposed $(n, n + 1)$-MSIS scheme is given in Algorithm 2.

4. Experimental Results and Analysis

In this section, experimental results and analysis of proposed $(n, n + 1)$-MSIS is done. The experiments are performed for grayscale and colored images. For binary images we have to make some changes in algorithm, modulus value should be updated as 2 with it, multiplication and division operator has to be taken off. Experimental results are performed on Intel(R) Core(TM) i7-4710HQ 2.50 Ghz Processor, 8GB RAM machine using MATLAB 13. All images are of size 512 × 512.

The experimental results of proposed $(n, n + 1)$-MSIS scheme for grayscale images are shown in Fig. 1. Input secrets images $SI_1, SI_2, SI_3, SI_4, SI_5$ are shown in Fig. 1(a)–(e) respectively. Fig. 1(f)–(k) shows noisy images

```
Input: n secret images $\{SI_1, SI_2 \cdots SI_n\}$ of size $h \times w$.
Output: $n + 1$ noisy images $\{NI_1, NI_2 \cdots NI_n, NI_{n+1}\}$.
  1. Generate n temporary Shares $\{C_1, C_2 \cdots C_n\}$ using round function.
       $C_i = round((SI_i/(n + 1)))$ , where $\{i = 1, 2, \ldots, n\}$
  2. Generate a Random Matrix R of size $h \times w$
       $R = Random(h, w)$
  3. Generate Server Side Key SK using additive modulo
       $SK = (C_1) mod\ 256$
       $SK = (C_i + SK) mod\ 256$, where $\{i = 2, 3, \ldots, n\}$
  4. Generate n + 1 Noisy images $\{NS_1, NS_2 \cdots NS_n, NS_n + 1\}$ using additive modulo
       $NI_i = (C_i + SK + R) mod\ 256$ where $\{i = 1, 2, \ldots, n\}$
       $NI_{n+1} = ((n + 1) \times (SK + R)) mod\ 256$
```

Algorithm 1. Proposed noisy share generation procedure

```
Input: $n + 1$ noisy images $\{N_1, N_2 \ldots N_n\}$.
Output: n recovered images $\{F_1, F_2 \ldots F_n\}$.
  1. Generate Client side key CK
       $CK = (N_1) mod\ 256$
       $CK = (CK + N_i) mod\ 256$, where $\{i = 2, 3 \ldots, n\}$
  2. Generate Temporary Noisy images
       $P_i = ((n + 1) \times N_i) mod\ 256$, where $\{i = 1, 2, \ldots, n\}$
  3. Generation of Random matrix R using additive inverse
       $R = (N_{n+1} - CK) mod\ 256$
  4. Generation of Recovered images$\{ F_i, i = 1, 2, \ldots, n\}$
       $F_i = (P_{n+1} - (CK + R)) mod\ 256$
```

Algorithm 2. Proposed recovery procedure

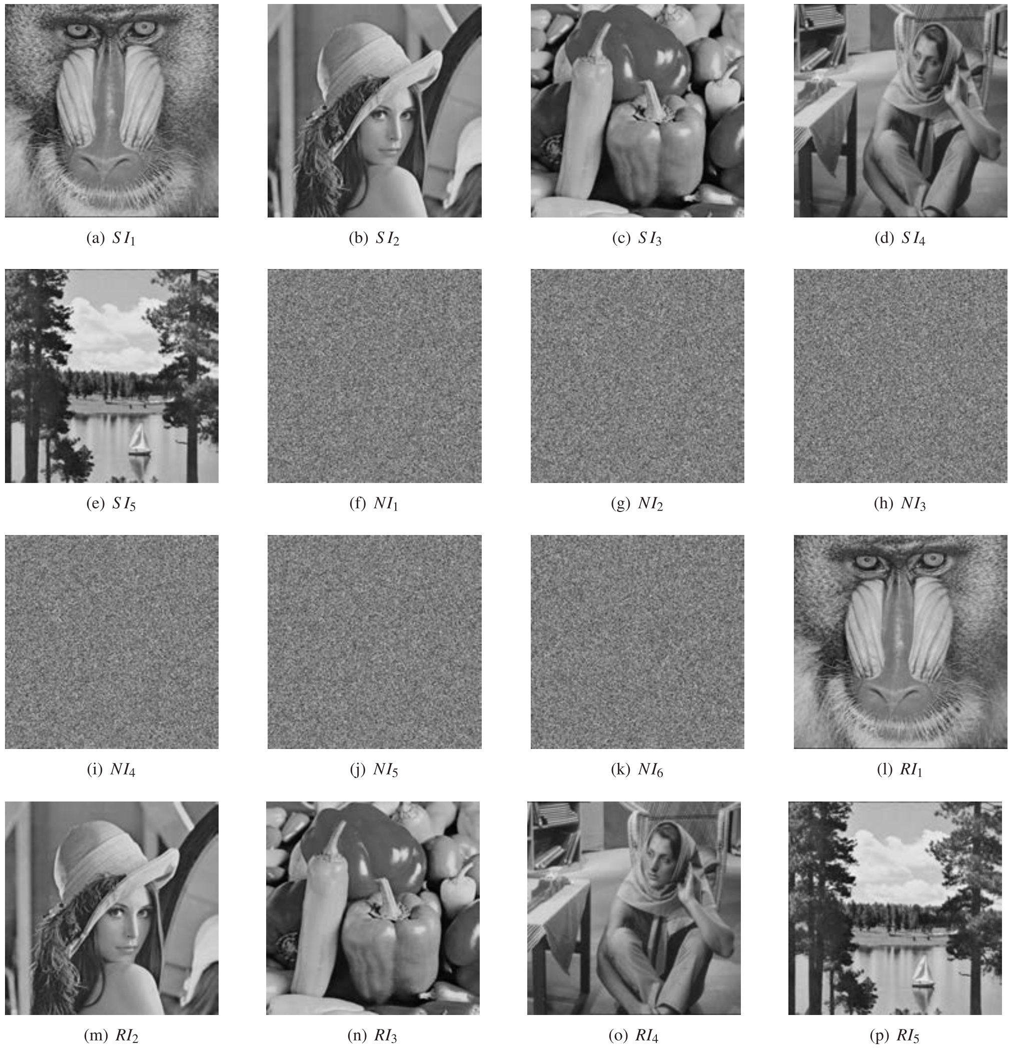


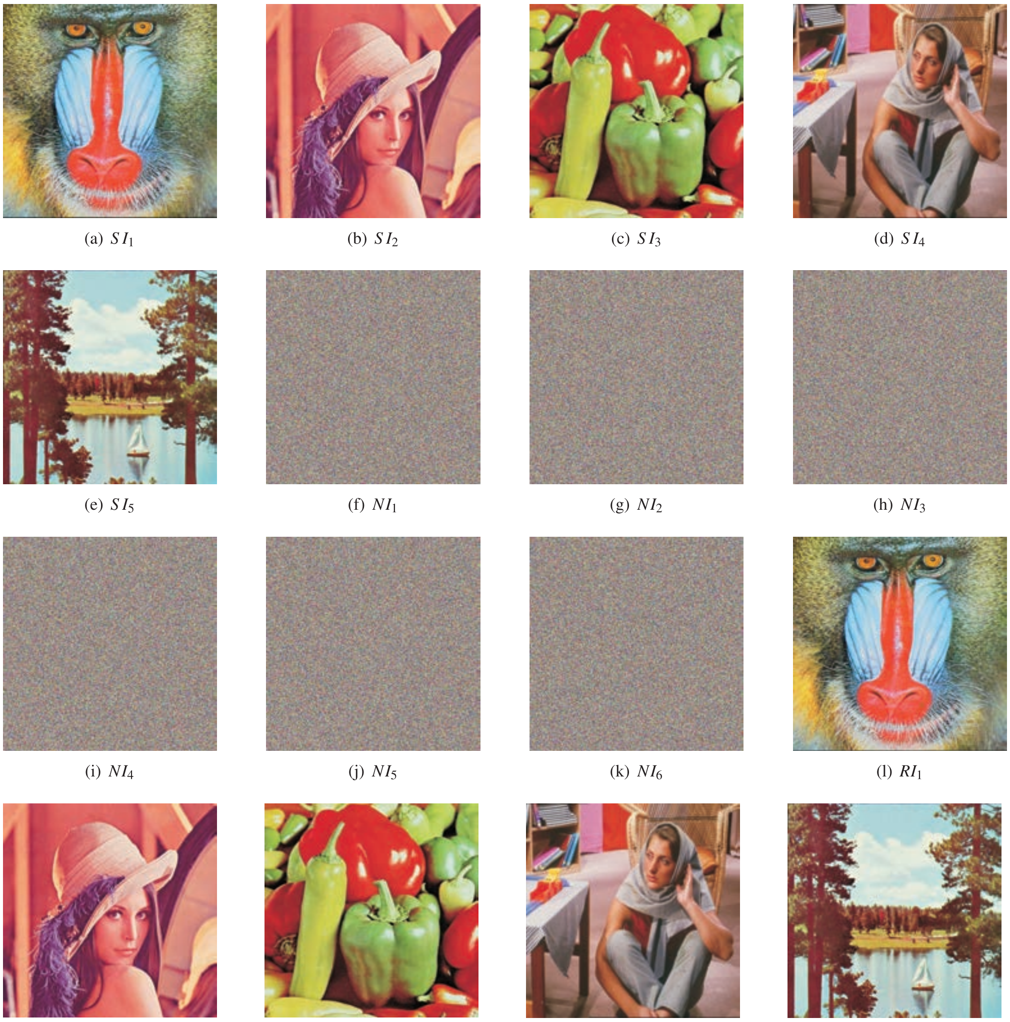
Fig. 1. Result of Proposed $(n, n+1)$-MSIS Scheme for Grayscale Images with $n = 5$: (a–e) Secret Images (SI_1, SI_2, SI_3, SI_4, SI_5); (f–k) Noisy Images (NI_1, NI_2, NI_3, NI_4, NI_5, NI_6); (l–p) Recovered Images (RI_1, RI_2, RI_3, RI_4, RI_5).

$NI_1, NI_2, NI_3, NI_4, NI_5, NI_6$ respectively. No share individually reveals any information of secret images. Figure 1(l)–(p) shows recovered images RI_1, RI_2, RI_3, RI_4, RI_5 which are almost similar to the secret images.

The experimental results of proposed $(n, n + 1)$-MSIS scheme for colored images are shown in Fig. 2. Input secrets images $SI_1, SI_2, SI_3, SI_4, SI_5$ are shown in Fig. 2(a)–(e) respectively. Fig. 2(f)–(k) shows noisy images $NI_1, NI_2, NI_3, NI_4, \ NI_5, NI_6$ respectively. No share individually reveals any information of secret images. Figure 2(l)–(p) show recovered images RI_1, RI_2, RI_3, RI_4, RI_5 and recovered images are almost similar to the secret images.

4.1 Quantitative Analysis

In quantitative analysis, similarity between secret and recovered images of proposed $(n, n + 1)$-MSIS scheme is done using Correlation, RMSE and PSNR. The results we get using different functions like floor, ceil and round are shown in Table 1.



(a) SI_1 (b) SI_2 (c) SI_3 (d) SI_4

(e) SI_5 (f) NI_1 (g) NI_2 (h) NI_3

(i) NI_4 (j) NI_5 (k) NI_6 (l) RI_1

(m) RI_2 (n) RI_3 (o) RI_4 (p) RI_5

Fig. 2. Result of Proposed $(n, n+1)$-MSIS Scheme for Color Images with $n = 5$: (a–e) Secret Images ($SI_1, SI_2, SI_3, SI_4, SI_5$); (f–k) Noisy Images ($NI_1, NI_2, NI_3, NI_4, NI_5, NI_6$); (l–p) Recovered Images ($RI_1, RI_2, RI_3, RI_4, RI_5$).

- **Correlation:** The correlation value lies between $+1$ and -1, $+1$ indicate that the two compared images are same, -1 indicate that both of them are opposite to each other and 0 if both are uncorrelated. Correlation is given as

$$\text{Correlation} = \frac{n\sum pq - (\sum p)(\sum q)}{\sqrt{(n\sum p^2 - (\sum p)^2)(n\sum q^2 - (\sum q)^2)}} \tag{1}$$

- **RMSE:** RMSE is the root mean squared error between the original image I and the compared image R. RMSE value tells the difference between two images. RMSE is given as

$$\text{RMSE} = \sqrt{\frac{1}{M \times N}\sum_{x=1}^{M}\sum_{y=1}^{N}(SI(x, y) - RI(x, y))^2} \tag{2}$$

Table 1. Comparison of Secret and Recovered Images of Proposed $(n, n+1)$-MSIS Scheme.

	FLOOR			CEIL			ROUND		
Secret and Recovered Images	Correlation	RMSE	PSNR	Correlation	RMSE	PSNR	Correlation	RMSE	PSNR
SI_1, RI_1	0.9992	3.0266	38.55 dB	0.9992	3.0288	38.54 dB	0.9992	1.7796	43.16 dB
SI_2, RI_2	0.9994	2.8873	38.96 dB	0.9994	3.1793	38.12 dB	0.9994	1.7796	43.10 dB
SI_3, RI_3	0.9995	3.0325	38.53 dB	0.9995	3.0270	38.54 dB	0.9995	1.7808	43.15 dB
SI_4, RI_4	0.9993	3.0230	38.56 dB	0.9993	3.0306	38.53 dB	0.9993	1.7808	43.15 dB
SI_5, RI_5	0.9997	3.0251	38.55 dB	0.9997	3.0293	38.54 dB	0.9997	1.7803	43.15 dB

Table 2. Analysis of Proposed $(n, n+1)$-MSIS Scheme.

Parameters	Proposed Scheme Results
Secret Images	n
Shared Images	$n+1$
Time(s)	0.329
Pixel Expansion	No
Reveal Secrets	No
Sharing Type	Rectangle
Sharing Capacity	$n/n+1$
Color Depth	Binary, Grayscale, Color
Recovery Strategy	Additive Modulo

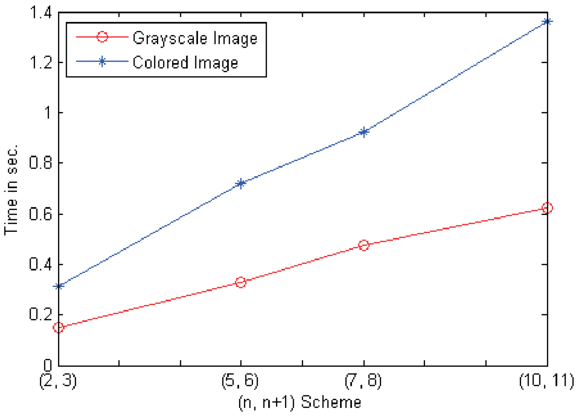


Fig. 3. Time Complexity of Proposed $(n, n+1)$ Scheme.

- **PSNR:** PSNR calculates the quality of the recovered images. The higher the PSNR better the quality and vice versa. The PSNR is given as:

$$\text{PSNR}(dB) = 20\log_{10}\frac{255}{\text{RMSE}} \tag{3}$$

  where, 255 is the highest pixel value in grayscale and colored images.

A complete analysis regarding performance of proposed $(n, n+1)$-MSIS scheme is given in Table 2. No pixel expansion is there as size of secret images, noisy images and recovered images are same. To reveal secrets all $n+1$ shares are needed. For making $(n, n+1)$-MSIS scheme work for binary images, some changes are to be made, like modulus value has to be updated as 2. No scalar multiplication and division is needed as it will lead to overflow of bits. Additive modulo is used for encryption and decryption. Sharing capacity of proposed scheme is $n/n+1$.

Time complexity of proposed $(n, n+1)$-MSIS scheme for grayscale and colored secret images is shown in Fig. 3. As we increase no of secret images *i.e. (value of n)* time required for execution also increase both for color and grayscale images. Computation time for colored image is more than binary and grayscale image because increase in number of bits. Time complexity of proposed scheme is high due to multiplication and division operations performed during encryption and decryption.

5. Conclusions

In this Paper, we overcome the security problem which was faced in[3–5] MSIS schemes. We used additive modulo operation which is faster than XOR operation. The proposed scheme shows better results in terms of security. Proposed scheme uses random matrix to generate randomness in shared images, so that stacking of less than $n + 1$ noisy images will not reveal any information of secret images. To check the similarity between secret and recovered images we used Correlation, RMSE and PSNR techniques.

6. Future Scope

Proposed scheme uses $n + 1$ noisy images to reconstruct n secret images which increases space as well as time complexity. We can try to reduce number of shares to make it more efficient than the existing one. Proposed scheme do not work if secret images are of different size. In future work this can be achieved so, MSIS scheme will not have any dependency on the size of secret images.

References

[1] Shamir and Adi, How to Share a Secret, *Communications of the ACM*, pp. 612–613, (1979).

[2] Naor, Moni and Adi Shamir, Visual Cryptography, *Advances in Cryptology EUROCRYPT'94*, Springer Berlin/Heidelberg, (1995).

[3] Chen, Tzung-Her and Chang-Sian Wu, Efficient Multi-Secret Image Sharing Based on Boolean Operations, *Signal Processing*, pp. 90–97, (2011).

[4] Chen, Chien-Chang and Wei-Jie Wu, A Secure Boolean-Based Multi-Secret Image Sharing Scheme, *Journal of Systems and Software*, vol. 92, pp. 107–114, (2014).

[5] Yang, Ching-Nung, Cheng-Hua Chen and Song-Ruei Cai, Enhanced Boolean-Based Multi Secret Image Sharing Scheme, *Journal of Systems and Software*, (2015).

[6] Wang, Daoshun, *et al.*, Two Secret Sharing Schemes Based on Boolean Operations, *Pattern Recognition*, pp. 2776–2785, (2007).

[7] Shyu and Shyong Jian, Image Encryption by Random Grids, *Pattern Recognition*, pp. 1014–1031, (2007).

[8] Chen, Tzung-Her and Kai-Hsiang Tsao, Threshold Visual Secret Sharing by Random Grids, *Journal of Systems and Software*, pp. 1197–1208, (2011).

[9] Maroti Deshmukh and Munaga V. N. K. Prasad, Comparative Study of Visual Secret Sharing Schemes to Protect Iris Image, *International Conference on Image and Signal Processing (ICISP)*, pp. 91–98, (2014).

[10] Lin, Kai-Siang, Chih-Hung Lin and Tzung-Her Chen, Distortionless Visual Multi-Secret Sharing Based on Random Grid, *Information Sciences*, vol. 288, pp. 330–346, (2014).