Secured Communication Method using Visual Secret Sharing Scheme for Color Images

John Blesswin A.[1], Selva Mary G.[2], Manoj Kumar S.[3]

[1] Computer Science and Engineering, K. Ramakrishnan College of Technology, India
[2] Information Technology, M. Kumarasamy College of Engineering, India
[3] Information Technology, Karpagam College of Engineering, India
johnblesswin.rnd@gmail.com, selvamaryg.rnd@gmail.com, callsmk@gmail.com

Abstract

Protecting Personally identifiable information (PII) and Protected health Information (PHI) is always challenging in this digital era. An ongoing global pandemic of coronavirus disease 2019 called as coronavirus pandemic (COVID-19), has forced people towards digital transaction of data all over the world. Telemedicine allows health care service providers to evaluate, diagnose and treat patients at a distance using telecommunications tools and technology. Patients communicate the medical reports, medical images and related documents by email. Data that carries PHI information, is communicated via public networks in the form of image and are vulnerable. An effective encryption technique is always in need to transfer such information securely. Visual Secret Sharing (VSS) scheme is an efficient encryption scheme that decodes the image by dividing into number of shares. Individual shares do not reveal any secret and stacking of all shares can reveal the secret image. In this article, Semantic Visual Secret Sharing scheme (SVSS) is proposed, which can be applicable for both gray-scale and color images. In this SVSS, the secret color image I is converted into semantic image SI by reducing the pixel errors. This SI decreases the encoding complexity without affecting the quality. The proposed SVSS avoids pixel expansion issues faced by traditional VSS schemes. Also, the Peak Signal-to-Noise Ratio (PSNR) value of the reconstructed secret color image shows better quality of the reconstructed secret image. The pixel errors that get introduced during share generation phase is reduced. The experimental result shows the effectiveness of the proposed SVSS and ensures secure transmission.

Keywords: Color image, Error reduction, Secret sharing, Visual cryptography

1 Introduction

Securing data over the Internet has become the important issue in the development of Information Systems. Identity Theft and Medical Identity theft can make more money than stealing credit card numbers or passwords. Health Insurance Portability and Accountability Act (HIPPA) regulates norms and policies to protect such information. Information are communicated in the form of Text or Images. Information shared in the form of images need more attention as, 70% of information is shared as image and traditional cryptography algorithms cost more for images. That is, any grayscale image of size 256×256 will have 65536 pixels. Traditional cryptography schemes such as Advanced Encryption Standard, symmetric or asymmetric schemes will be tedious to be applied on such large data. Visual Secret Sharing (VSS) scheme is the new encryption technique to transfer the images securely. VSS functions include, share construction phase and revealing phase. In the share construction phase, the Secret Image (*SI*) is encoded and are divided into (*n*) number of share images. Individual share images do not contain any information about the secret image. The secret image can be visually revealed by digitally stacking all the shares using logical XOR operation.

In the study of previous research articles, the following conclusions are listed: Multiple shares are generated using black and white pixel values based on the secret image pixel [1]. Each pixel is replaced by subpixel/subpixels that increases the size of the shares [2-3]. Schemes are applied on color images that increases the cost of computations [4]. Color VSS schemes uses color index table in the revealing phase [5-7]. VSS schemes produces binary shares. Preprocessing of images such as half-toning increases the cost for computations. Pixel expansion issues becomes challenging to security [8-10]. Color VSS schemes used key shares and are protected by generating random shares; Natural cover images used for hiding noise-like shares [11]; Digitally stacking up of shares using logical XOR operations revealed secret images [12-13].

The proposed Semantic Visual Secret Sharing

*Corresponding Author: Selva Mary G.; E-mail: selvamaryg.rnd@gmail.com
DOI: 10.53106/160792642021072204008

scheme (SVSS) focuses on three paths,

1. High quality reconstructed secret image
2. Secret image sharing with less computational complexity
3. No pixel expansion on shares and shares to look like any natural images

This article is structured as follows: Section 2, explains the error reduction technique, which is adapted in proposed SVSS. Proposed SVSS algorithm and its explanation are explained in Section 3. Further Section 4 gives experimental results and its discussions. Conclusions are listed out in Section 5.

2 Semantic Image Generation

The secret color image I is converted into semantic image SI. The pixels are converted into meaningful pixel values. The semantic image generated will have pixel values ranges from $SI \in \{0, 1, 2, ..., 252\}$. The semantic image pixel values are discrete in nature and are having similar values to the adjacent pixel values. This forms a cluster of pixel values. Figure 1 shows the work flow of semantic image generation from the secret image.

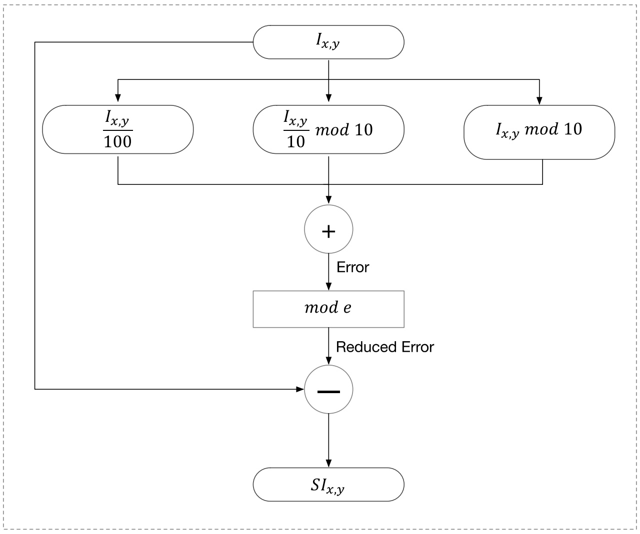


Figure 1. Semantic Image Generation

Figure 1 explains the following steps to convert the secret image into semantic image. Initially, the secret color image is separated in to three channels Red (R), Green (G) and Blue (B). Each channel pixel values ranges from 0 to 255. In the proposed SVSS each channel is processed individually. Each pixel in each of the channel is processed to convert into semantic pixel with the following steps:

Step1: The pixel error is calculated from each individual pixel. This step helps to get the coefficients of the pixel in integer form.

Step 2: The semantic image SI is generated by reducing the pixel errors. Pixel Error (E) is calculated to all the pixels and are reduced from the original pixel values [10]. Reducing this error from the pixel provides a meaning to the pixels. The threshold value (e) of any error is limited to 9. $e$is chosen to get the digit sum. The digit sum function $digitsum(k) = (k-1)\%9+1$.

Step 3: In the proposed SVSS the value of $E$is reduced further.

Step 4: Minimizing the reduced error from the original pixel value generates a meaningful pixel. The quality of the semantic image is maintained and improved with this reduced error.

Figure 2 shows the comparative analysis of sample Lena secret color image with semantic image generated. The semantic image SI green channel (G) has clusters of same pixel values when compare to secret image I green channel (G). The quality of the SI is reduced compared to the I; However, the luminance is not lost.

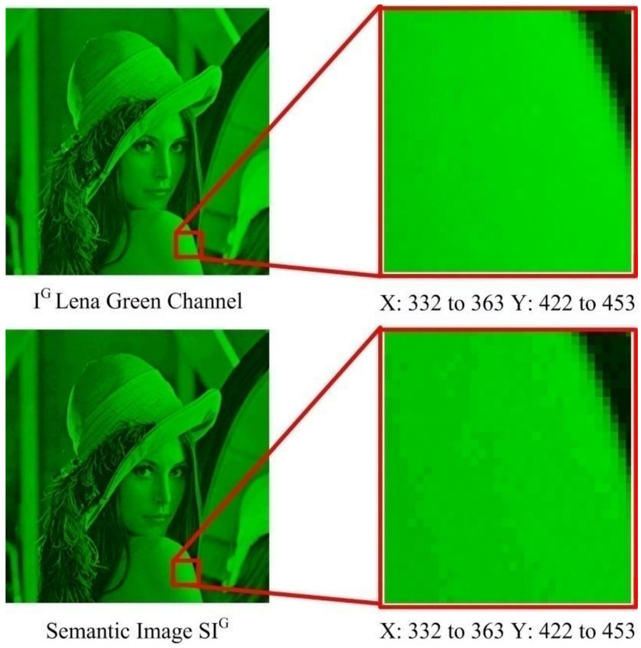


Figure 2. Comparison of Lena Secret image I and semantic image SI

Algorithm 1 shows the step by step process of semantic image generation from the secret image.

Algorithm 1. Generation of semantic image

Input: Secret color Image I^{RGB} *of size* $M \times N$ *of RGB channels*

Output: Semantic Image SI^{RGB} *of size* $M \times N$ *of RGB channels*

$I^R, I^G, I^B \leftarrow RGB \leftarrow I^{RGB}$

For each channel R, G, B of I,

For each $x \leftarrow 1 : M$

For each $y \leftarrow 1 : N$

do until $(x \leftarrow M \,\&\, y \leftarrow N)$

$E_{(x,y)} \leftarrow \left(\frac{I_{(x,y)}}{100} + \frac{I_{(x,y)}}{10} \bmod 10 + I_{(x,y)} \bmod 10\right)$

$RE_{(x,y)} \leftarrow E_{(x,y)} \bmod e$

$SI^R_{(x,y)} \leftarrow I^R_{(x,y)} - RE^R_{(x,y)}$

$SI^G_{(x,y)} \leftarrow I^G_{(x,y)} - RE^G_{(x,y)}$

$SI^B_{(x,y)} \leftarrow I^B_{(x,y)} - RE^B_{(x,y)}$

$SI^{RGB} \leftarrow RGB \leftarrow I^R, I^G, I^B$

3 Proposed Semantic Visual Secret Sharing Scheme

This section presents a detailed description of the proposed *SVSS* The proposed SVSS encodes the secret image and divide into Intermediate Share (*IS*) images. The cover images are used to hide the *IS*. The covered *IS* images are called share images. In the proposed *SVSS*, a semantic image *SI* is created from the color secret image *I* sized *M*×*N* pixel values, by using semantic image generation technique. The *SVSS* functions are firstly, sharing and embedding phase, which creates two shares from the secret image *I*. *IS*1 and *IS*2 will be covered by natural cover images *C*1 and *C*2. Secondly, in the revealing phase, the secret image is revealed as reconstructed Secret Image (*RI*) from the shares *S*1 and *S*1. Even if one of the shares is lost, the secret image cannot be revealed.

3.1 Share Construction Phase

A detailed algorithm for the sharing and embedding phase also called as share construction phase is described in this section. A general flowchart of the sharing and embedding phase of our scheme appears in Figure 3. The secret color image *I* is decomposed into Red (I^R), Green (I^G) and Blue (I^B) channels.

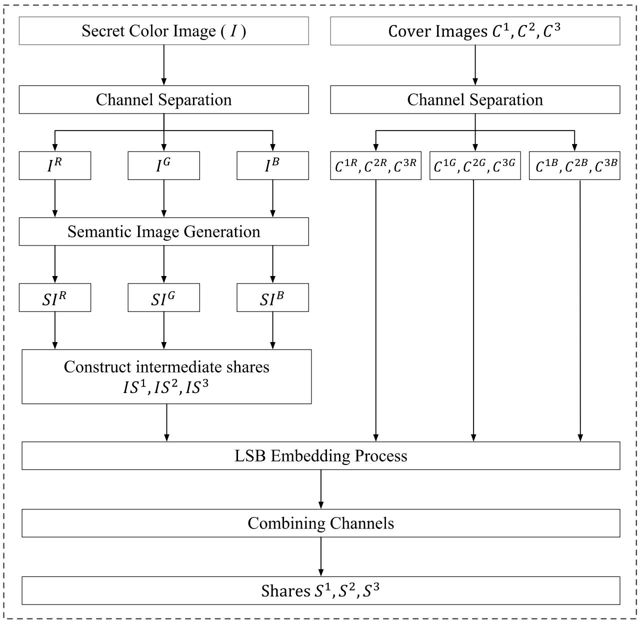


Figure 3. Share construction and embedding phase

Figure 3 shows the step by step procedure of share construction phase. In this phase, the secret color image I is separated into red, green and blue channels I^R, I^G, I^B. The semantic image is generated using Algorithm 1. The algorithm to generate the shares are depicted in Algorithm 2.

Algorithm 2. Share generation phase

Input: Secret color Image I^{RGB}, Cover images C^1, C^2, C^3 are of size $M \times N$ of RGB channels.

Output: Shares S_1^{RGB}, S_2^{RGB} *of size* $M \times N$ *of RGB channels*

$SI^{RGB} \leftarrow$ *Semantic image generation* $\leftarrow I^{RGB}$

For each channel R, G, B of SI, C^1, C^2, C^3

For each $x \leftarrow 1 : M$

For each $y \leftarrow 1 : N$

do until $(x \leftarrow M \; \& \; y \leftarrow N)$

$IS^1_{(x,y)} \leftarrow \frac{SI_{(x,y)}}{100}$

$IS^2_{(x,y)} \leftarrow rand(0,1)$

$IS^3_{(x,y)} \leftarrow \begin{cases} SI_{(x,y)} \bmod 10, & IS^2_{(x,y)} = 1 \\ \frac{SI_{(x,y)}}{10} \bmod 10, & IS^2_{(x,y)} = 0 \end{cases}$

$S^1_{(x,y)} \leftarrow C^1_{(x,y)} - \left(C^1_{(x,y)} \bmod 10\right) + IS^1_{(x,y)}$

$S^2_{(x,y)} \leftarrow C^2_{(x,y)} - \left(C^2_{(x,y)} \bmod 10\right) + IS^2_{(x,y)}$

$S^3_{(x,y)} \leftarrow C^3_{(x,y)} - \left(C^3_{(x,y)} \bmod 10\right) + IS^3_{(x,y)}$

End do

End For

End For

Algorithm 2 explains the working of the share construction phase of the proposed SVSS. Initially the secret color image I is converted in to semantic image SI. Secondly, SI is encoded and are divided in to intermediate shares IS^1, IS^2, IS^3. The coefficients of the SI pixel are randomly chosen. Thirdly, the shares S^1, S^2, S^3 are generated by embedding the IS^1, IS^2, IS^3 on the cover images C^1, C^2, C^3 using Least Significant Bit (LSB) embedding process [14]. The generated shares are communicated to the authorized participants through the communication channel, any third-party software or mail clients etc. The intermediate shares ranges as, $IS^1 \in \{0,1,2\}, IS^2 \in \{0,1\}, IS^3 \in \{0,1,2,...,9\}$. The shares ranges as, $S^1, S^2, S^3 \in \{0,1,2,...,255\}$.

3.2 Revealing Phase

This section describes the proposed secret reconstruction or revealing phase of the proposed SVSS. A general flowchart of the revealing phase of SVSS appears in Figure 4. Figure 4 shows that, initially, the received shares are separated as R, G, B channels for processing. Each channel of shares has undergone the LSB extraction process and the Reconstructed Intermediate Shares (RIS^1, RIS^2, RIS^3) are obtained [15]. Secondly, a *key*is generated from the received *RIS*The threshold error value *e*is set as 9. Later, the reconstructed Semantic Image pixel values *RSI*are decoded using the retrieved *RIS* and the key generated. The RSI is obtained by digitally stacking all the retrieved shares and the key and by combining the R, G, B channels.

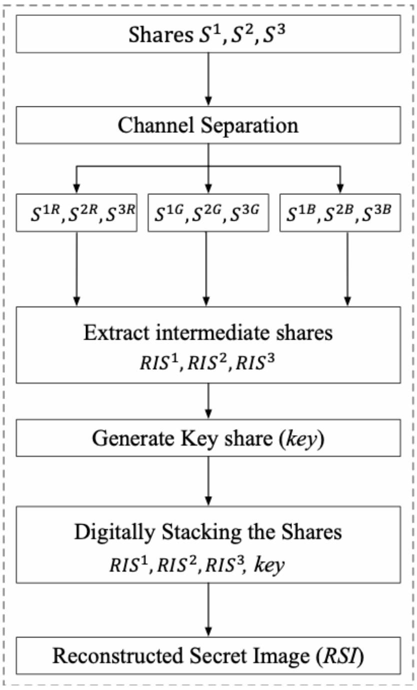


Figure 4. Revealing phase

The working principles of the revealing phase is depicted in Algorithm 3.

Algorithm 3. Revealing phase

Input: Share Image S^1, S^2, S^3 *are of size* $M \times N$ *of RGB channels.*
Output: Reconstructed Semantic Image RSI of size $M \times N$ *of RGB channels*
For each channel R, G, B of S^1, S^2, S^3
For each $x \leftarrow 1 : M$
For each $y \leftarrow 1 : N$
do until $(x \leftarrow M \,\&\, y \leftarrow N)$
$RIS^1_{(x,y)} \leftarrow S^1_{(x,y)} \bmod 10$
$RIS^2_{(x,y)} \leftarrow S^2_{(x,y)} \bmod 10$
$RIS^3_{(x,y)} \leftarrow S^3_{(x,y)} \bmod 10$
$key_{(x,y)} \leftarrow TH - (RIS^1_{(x,y)} + RIS^3_{(x,y)})$
$RSI_{(x,y)} \leftarrow \begin{cases} RIS^1_{(x,y)} \times 100 + RIS^3_{(x,y)} \times 10 + key_{(x,y)}, & RIS^2_{(x,y)} = 0 \\ RIS^1_{(x,y)} \times 100 + key_{(x,y)} \times 10 + RIS^3_{(x,y)}, & RIS^2_{(x,y)} = 1 \end{cases}$
End do
End For
End For

Table 1. Working model of proposed SVSS share generation for 8×8 size

245	59	162	150	250	176	61	100
54	186	219	164	201	73	80	156
64	26	174	48	247	156	247	54
136	152	80	48	47	213	201	143
231	42	73	244	194	19	43	34
139	182	231	63	174	181	247	50
75	37	3	121	48	173	241	172
211	61	183	115	200	186	72	215

(a) Secret Image I^R

2	5	0	6	7	5	7	1
0	6	3	2	3	1	8	3
1	8	3	3	4	3	4	0
1	8	8	3	2	6	3	8
6	6	1	1	5	1	7	7
4	2	6	0	3	1	4	5
3	1	3	4	3	2	7	1
4	7	3	7	2	6	0	8

(b) Reduced Error E

243	54	162	144	243	171	54	99
54	180	216	162	198	72	72	153
63	18	171	45	243	153	243	54
135	144	72	45	45	207	198	135
225	36	72	243	189	18	36	27
135	180	225	63	171	180	243	45
72	36	0	117	45	171	234	171
207	54	180	108	198	180	72	207

(c) Semantic Image SI^R

2	0	1	1	2	1	0	0
0	1	2	1	1	0	0	1
0	0	1	0	2	1	2	0
1	1	0	0	0	2	1	1
2	0	0	2	1	0	0	0
1	1	2	0	1	1	2	0
0	0	0	1	0	1	2	1
2	0	1	1	1	1	0	2

(d) Intermediate share IS^1

1	1	0	1	0	0	0	0
0	1	0	1	1	0	1	0
1	0	0	1	0	0	1	1
1	0	0	0	0	1	1	1
0	1	0	0	0	1	1	1
0	0	1	1	1	1	0	1
0	0	0	0	0	0	1	0
1	1	1	0	0	0	0	0

(e) Intermediate share IS^2

3	4	6	4	4	7	5	9
5	0	1	2	2	7	2	5
3	1	7	5	5	5	3	4
5	4	7	4	4	7	8	5
2	6	7	4	4	8	6	7
3	8	5	3	3	0	4	5
7	3	0	1	1	7	4	7
7	4	0	0	0	8	7	0

(f) Intermediate share IS^3

241	86	10	22	14	147	119	78
232	0	167	28	220	99	213	160
15	213	192	102	79	52	129	38
19	196	32	109	93	119	205	167
25	125	89	13	59	184	55	221
102	61	27	75	237	175	27	163
179	151	94	63	252	229	11	84
180	191	144	203	210	7	34	83

(g) Cover Image C^{1R}

65	45	73	12	83	169	137	15
37	247	236	85	89	19	57	145
81	87	61	78	186	175	5	162
189	53	173	229	2	249	75	106
66	40	158	155	155	205	3	36
216	42	26	95	231	251	7	163
157	75	143	237	82	93	221	75
100	224	226	132	76	182	60	195

(h) Cover Image C^{2R}

188	205	244	34	89	219	196	197
200	112	103	192	159	116	64	32
8	9	133	36	192	42	93	113
173	122	40	90	245	46	197	57
21	227	171	11	35	26	216	189
196	238	204	106	253	236	117	221
146	133	219	240	81	55	74	151
67	92	28	80	175	215	233	61

(i) Cover Image C^{3R}

242	80	11	21	12	141	110	70
230	1	162	21	221	90	210	161
10	210	191	100	72	51	122	30
11	191	30	100	90	112	201	161
22	120	80	12	51	180	50	220
101	61	22	70	231	171	22	160
170	150	90	61	250	221	12	81
182	190	141	201	211	1	30	82

(j) Share Image S^{1R}

61	41	70	11	80	160	130	10
30	241	230	81	81	10	51	140
81	80	60	71	180	170	1	161
181	50	170	220	0	241	71	101
60	41	150	150	150	201	1	31
210	40	21	91	231	251	0	161
150	70	140	230	80	90	221	70
101	221	221	130	70	180	60	190

(k) Share Image S^{2R}

183	204	246	34	84	217	195	199
205	110	101	192	158	117	62	35
3	1	137	35	194	45	93	114
175	124	47	94	244	47	198	55
22	226	177	14	38	28	216	187
193	238	205	103	251	230	114	225
147	133	210	241	84	57	74	157
67	94	20	80	179	218	237	60

(l) Share Image S^{2R}

The algorithm depicted in this revealing phase uses simple computations to decrypt the *RSI*. Any of the faked, modified or corrupted share do not reveal the *RSI*

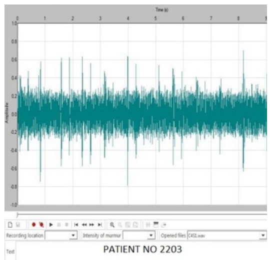
The working model of the proposed algorithm is explained with a sample 8×8 sized matrix values of a single Red channel of the *I*. Table 1 shows the working model of the share generation phase.

4 Experimental Results and Analysis

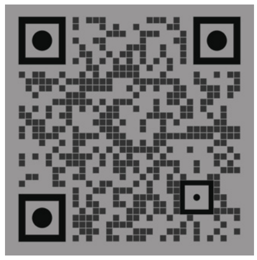
Experimental results demonstrate on three objectives. Firstly, reconstructed secret image with high quality; secondly, corresponding to reduced complexity; lastly, relating with no pixel expansion. The proposed SVSS can be applied on any sized secret color images. The efficiency of the proposed method outlined in this research work is tested by coding and running the algorithm in MATLAB 7.10 Tool. The image quality measures are evaluated between reconstructed images and original secret images. The set of test images considered as medical images and Quick Response (QR) images are shown in Figure 5. Figure 6 shows that the set of cover images used for experimental analysis. These images are chosen from the set of sample MATLAB images. The cover images can be of any image of size same as of secret image. The proposed SVSS is tested with more than 80 sample test images of various types such as, medical images, natural images and QR code images.

(a) Secret image 1

(b) Secret image 2

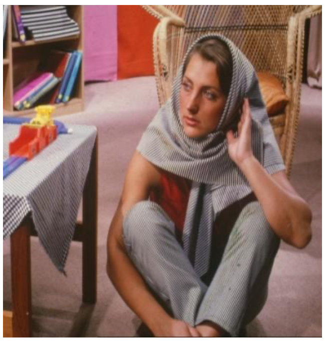


(c) Secret image 3



(d) Secret image 4

Figure 5. Sample secret images



(a) Cover image 1

(b) Cover image 1

(c) Cover image 3

Figure 6. Sample cover images

4.1 Test Analysis

Image quality is measured using the performance metrics such as, PSNR, SSIM, MSE and MAE. The original secret image and the reconstructed image is compared and the values are recorded. Table 1 shows the process of the secret images using proposed SVSS.

Figure 7 shows the individual shares do not reveal any secret information and are looking like any natural image. Thus, the share values are covered as meaningful shares.

PSNR: The term peak signal-to-noise ratio (PSNR) is the measured as a ratio between the maximum possible pixel value of the image and the value of noise that distresses the quality of its representation. It measures in terms of decibels (dB). Any PSNR greater than 25dB is considered as good and acceptable quality of the image [16].

SSIM: The structural similarity index measure (SSIM) is predicting the perceived quality of the image. SSIM values ranges between 0 to 1 where 0 means the dissimilarity between the images. Generally, SSIM values greater than 0.85 is represented for good quality reconstruction techniques [17].

MSE: The mean square error (MSE) measures the errors in the pixel values as average of the squares of the errors between pixels of the original and reconstructed image.

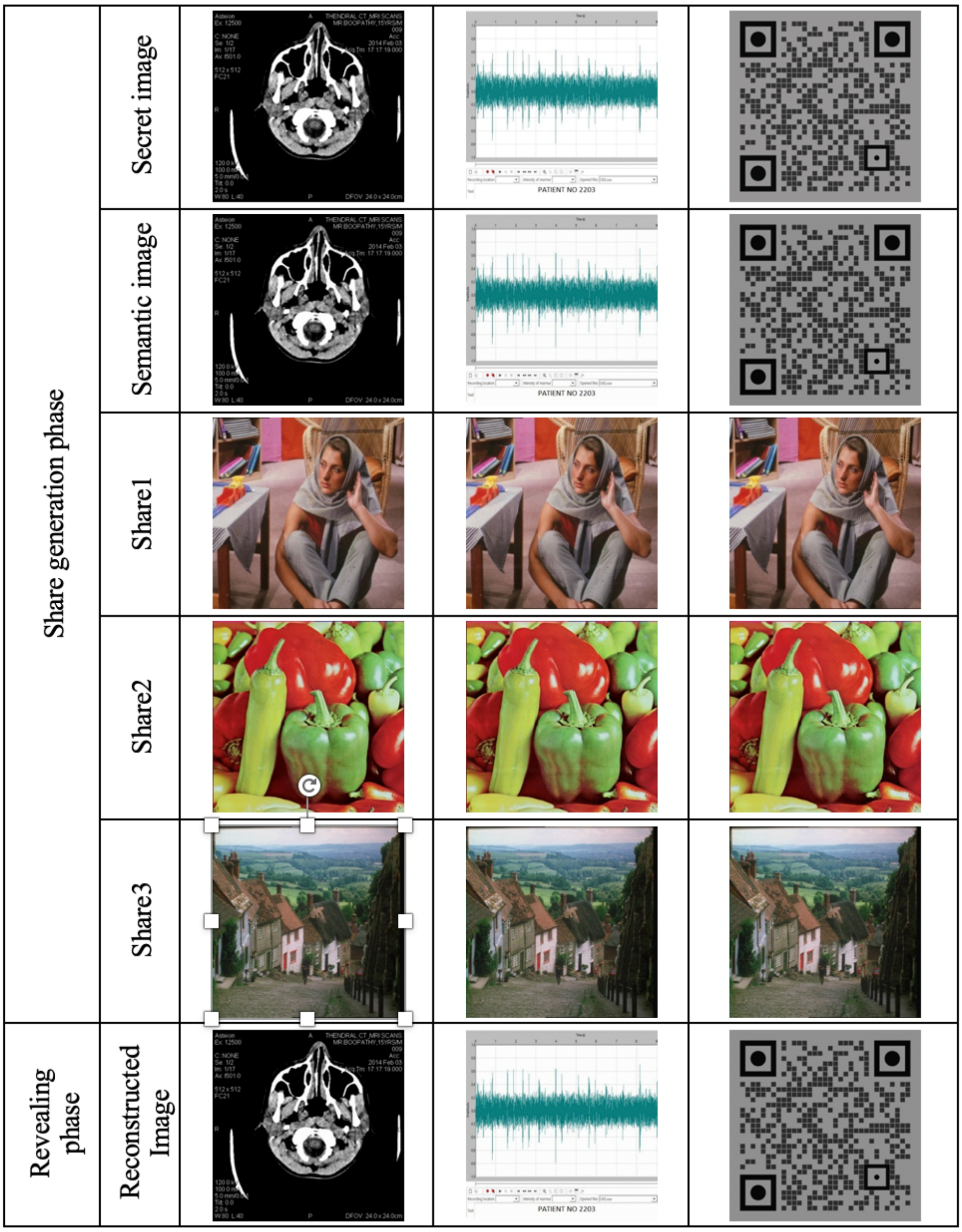


Figure 7. Image lifecycle in proposed SVSS

MAE: The mean absolute error (MAE) is a measure of distractions between observations.

The quality of the shares is measured and are listed in Table 1.

Table 2. Quality Measures of Secret Image Vs reconstructed image

Secret Images	PSNR	SSIM	MSE	MAE
Secret 1	40.242	0.926	6.148	3.560
Secret 2	36.905	0.867	13.25	9.482
Secret 3	38.581	0.956	9.644	6.996
Secret 4	33.195	0.615	22.220	14.280

From Table 2, it is observed that the quality of the reconstructed image is good and are in acceptable range.

Firstly, the security of the shares is ensured by randomly generating shares in the share generation phase. Secondly, a *key* share is generated from the received shares in the receiving end. The *key share* is used to decrypt the share. If any of the share is faked or altered, then the key share would not reconstruct the secret message. Thirdly, better quality of shares is maintained in this proposed scheme, hence, the chances for presume the secret is reduced. Finally, even if all the shares are accessed by any unauthorized parties, without the revealing phase, the secret cannot be reconstructed.

Table 3 compares the proposed SVSS with the existing schemes. The comparisons made based on the following criteria.

Number of shares (Check 1): The value n is the total number of shares generated using proposed SVSS.

PSNR value of reconstructed secret image (Check 2): This value is used to calculate the similarity of two images.

Shares generation (Check 3): It specifies technique adopted to generate shares [18].

Shares size (Check 4): The size of the secret color image *I*and size of the shares are compared.

Computational complexity (Check 5): It specifies the execution time for the performed operations with time complexity O(n).

Pixel Expansion (Check 6): It specifies the change in pixel size during share generation phase [19].

Table 3 shows that the proposed SVSS is efficient for the secure transmission of color images. The proposed SVSS shows higher the PSNR value than the existing schemes. In the proposed SVSS the secret image I is converted into semantic image SI, in order to avoid the pixel errors raised in share construction phase [20]. Thus, the quality is maintained. The proposed SVSS shows no pixel expansion while generating shares. Also, the proposed SVSS reduce the computational complexity by using simple arithmetic calculations while generating shares and revealing the reconstructed secret image. The proposed SVSS maintains its security of the share images by embedding into the cover images. Individual shares do not reveal the secret. Even if any intruder access all the shares, without the revealing phase, the secret cannot be restored. This section explains that the proposed SVSS is efficient scheme to transfer the secret color image with minimal computation and to maintain the quality of the images.

Table 3. Comparative analysis of proposed SVSS with existing schemes

Scheme	[3]	[4]	[7]	[9] & [15]	Proposed SVSS
Check 1	$n \geq 2$	$n \geq 2$	$n \geq 2$	$n = 2$	$n = 3$
Check 2	20-25dB	20-27dB	20-25dB	25-35dB	30-40dB
Check 3	Pixel replacement	Random based	Pixel replacement	Linear order	Random based
Check 4	$(2n+1) \times N$	$N \times 1.15$	$(2n+n+1) \times N$	N	N
Check 5	Very High	Medium	High	Low	Low
Check 6	≥ 1	≥ 1	≥ 2	Nil	Nil

5 Conclusion

In this Covid'19 era, most of the confidential information communicated via open networks in the form of images face security issues. The proposed SVSS scheme aims to maintain the quality of the reconstructed secret image without compromising the security features. The proposed SVSS converts the secret image into semantic image by reducing the pixel error. This improves the quality of the reconstructed image. Individual shares do not reveal any information of secret image Also, the proposed SVSS ensures no pixel expansion issues and minimal computational complexity. The proposed SVSS ensures that the technique is efficient for color images. It can also be very well used for grayscale and binary image.

References

[1] M. Naor, A. Shamir, Visual cryptography, in: A. De Santis (Eds.), *Advances in Cryptology-EUROCRYPT'94, Lecture Notes in Computer Science*, Vol. 950, Springer, Berlin, Heidelberg, 1994, pp. 1-12.

[2] E. R. Verheul, H. C. A. Van Tilborg, Constructions and Properties of k out of n Visual Secret Sharing Schemes, *Designs, Codes and Cryptography*, Vol. 11, No. 2, pp. 179-196, May, 1997.

[3] B. Yan, Y. Xiang, G. Hua, Improving the visual quality of size-invariant visual cryptography for grayscale images: an analysis-by-synthesis (AbS) approach, *IEEE Transactions on Image Processing*, Vol. 28, No. 2, pp. 896-911, February, 2019.

[4] H. Hua, Y. Liu, Y. Wang, D. Chang, Q. Leng, Visual Cryptography Based Multilevel Protection Scheme for Visualization of Network Security Situation, *Procedia Computer Science*, Vol. 131, pp. 204-212, 2018.

[5] M. Deshmukh, N. Nain, M. Ahmed, Efficient and secure multi secret sharing schemes based on Boolean XOR and arithmetic modulo, *Multimedia Tools and Applications*, Vol. 77, No. 1, pp. 89-107, January, 2018.

[6] C. Yang, C. Laih, New Colored Visual Secret Sharing Schemes, *Designs, Codes and cryptography*, Vol. 20, No. 3, pp. 325-336, July, 2000.

[7] C. Chang, C. Tsai, T. Chen, A New Scheme for Sharing Secret Color Images in Computer Network, *Proceedings of International Conference on Parallel and Distributed Systems*, Iwate, Japan, 2000, pp. 21-27.

[8] D. Jin, W. Yan, M. S. Kankanhalli, Progressive color visual cryptography, *Journal of Electronic Imaging*, Vol. 14, No. 3, Article No. 033019, July, 2005.

[9] R. Prisco, A. Santis, On the Relation of Random Grid and Deterministic Visual Cryptography, *IEEE Transactions on Information Forensics and Security*, Vol. 9, No. 4, pp. 653-665, April, 2014.

[10] S. J. Shyu, Efficient Visual Secret Sharing Scheme for Color Images, *Pattern Recognition*, Vol. 39, No. 5, pp. 866-880, May, 2006.

[11] J. Blesswin, P. Visalakshi, Optimal Visual Secret Sharing on Electrocardiography Images for Medical Secret Communications, *International Journal of Control Theory and Applications*, Vol. 9, No. 2, pp. 1055-1062, January, 2016.

[12] A. K. Chattopadhyay, A. Nag, J. P. Singh, A. K. Singh, A verifiable multi-secret image sharing scheme using XOR operation and hash function, *Multimedia Tools and Applications*, pp. 1-30, 2020.

[13] J. Fridrich, *Steganography in Digital Media: Principles, Algorithms, and Applications*, Cambridge University Press, Cambridge, England, 2014.

[14] J. Blesswin, P. Visalakshi, A Novel Visual Image Confirmation (VIC) Protocol Using Visual Cryptography for Securing Ubiquitous Bluetooth Mobile Communications, *Research Journal of Applied Sciences*, Vol. 9, No. 8, pp. 503-510, August, 2014.

[15] H. Kumar, A. Srivastava, A secret sharing scheme for secure transmission of color images, *International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT)*, Ghaziabad, India, 2014, pp. 857-860.

[16] J. Blesswin, P. Visalakshi, Multi-Secret Semantic Visual Cryptographic Protocol (MSVCP) for Securing Image Communications, *Asian Journal of Information Technology*, Vol. 13, No. 9, pp. 506-512, September, 2014.

[17] J. Blesswin, A. Genitha, G. Selvamary, A novelQR-code authentication protocol using visual cryptography for secure communications, *International Journal of Control Theory and Applications*, Vol. 9, No. 2, pp. 967-974, January, 2016.

[18] M. Gayathri, A. J. Blesswin, G. S. Mary, An Efficient QR-code Authentication Protocol using Visual Cryptography for Securing Ubiquitous Multimedia Communications, *Indian Journal of Science and Technology*, Vol. 9, No. 39, pp. 1-7, October, 2016.

[19] G. S. Mary, S. M. Kumar, Secure grayscale image communication using significant visual cryptography scheme in real time applications, *Multimedia Tools and Applications*, Vol. 79, No. 15-16, pp. 10363-10382, April, 2020.

[20] G. S. Mary, S. M. Kumar, A self-verifiable computational visual cryptographic protocol for secure two-dimensional image communication, *Measurement Science and Technology*, Vol. 30, No. 12, Article No. 125404, December, 2019.

Biographies

John Blesswin A. is an Assistant Professor, Computer Science & Engineering, K.Ramakrishnan College of Technology, Anna University, India. He received his B.E and M.Tech from Karunya University, India in 2009 and 2011 respectively. He received his Ph.D. degree from Anna University, India in 2018. His main research interests include visual cryptography, image communication.

Selva Mary G. is a Ph.D. research scholar in the Faculty of Information Communication Engineering, Centre for Research, Anna University, India. She received the B.E. degree in Computer Science and Engineering from Anna University, Chennai, India and M.E degree in Computer Engineering from University of Mumbai, India, in 2005 and 2014 respectively. Her research interests include visual cryptography, secret image sharing, and image communication.

Manoj Kumar S. is a Professor and Head in the Department of Information Technology, Karpagam College of Engineering, India. He received the B.E. in 2002 and M.E. in 2008, Computer Science and Engineering from Bharadhidasan University, and Anna University India respectively. He received Ph.D. degree from Anna University, Chennai, India in 2016. His research in Wireless Sensor Networks, IoT, Networking, visual cryptography and image security.