A Novel Progressive Visual Cryptography Approach with Chaotic Map for Securing Digital Contents

Dhiraj Pandey, Uma Shankar Rawat
JSS Academy of Technical Education
Noida
Manipal University, Jaipur
India
dhip2@yahoo.co.in, umashankar.rawat@jaipur.manipal.edu

ABSTRACT: *Progressive Visual Cryptography (PVC) is quite suitable for sharing sensitive digital data where, as the number of stacked share increases, more black regions will be decrypted. Over the past few years, designing of progressive visual recovery technique has been studied by many researchers. Previous research on PVC, such as Fang et al. (2006) and W.P.Fang et al. (2008) were all carrying pixel-expansion problem and also gives a poor visual quality on the recovered stacked image. Recently, Hou et al. have developed a progressive scheme for secret sharing. In Hou et al. scheme, secret object bits are encrypted sequentially by using randomly chosen number from encoding matrices. It is observed that shares generated by the Hou scheme are free from pixel expansion problem, but shares are not fully secure and even discloses secret itself in construction phase of encoding. In this paper, we propose a new robust progressive algorithm based on logistic chaotic map to overcome the said limitation of Hou scheme. The irregular outputs of the logistic map are used to encode a secret digital information carrying image. To provide robustness during the encoding process of the share, noise has been introduced along with chaotic sequences. The performance of the algorithm in the scheme of Hou is critically analyzed and compared with new suggested scheme. Empirical results are presented to showcase the performance of our proposed scheme in terms of its effectiveness (imperceptibility and security) and feasibility.*

Keywords: Progressive Visual Cryptography, digital Secret Sharing, Visual Cryptography, Unexpanded Shares, Logistic Map

Received: 18 September 2015, Revised 20 October 2015, Accepted 28 October 2015

1. Introduction

Research into the making digital content secure has been steadily growing. Conventional security techniques takes more computational time and space compare to visual cryptography based approach of securing data. A large number of visual cryptography techniques have appeared in the literature, for example [1-4]. These techniques can be divided into two main classes: traditional visual cryptography (TVC) and the progressive visual cryptography (PVC). Traditional approach has been widely studied by many researchers and suggested variants of strategy for protecting the content. A common drawback of using TVC based technique is the loss of contrast and pixel expansion problem. One may overcome issue of TVC using PVC based approaches. Concept emerged as "Progressive Visual Cryptography" has been explored by many researchers. The main objective of this paper is to investigate the security nature of existing schemes along with the feasibility of using chaotic map or improving security in shares of PVC. A chaotic response can be generated by applying periodic force to a nonlinear system. A computational framework for digital implementation of dynamic visual cryptography based on chaotic oscillations is presented by many researchers [5], but an effective experimental implementation of a chaotic progressive visual cryptography remains an open question in the literature.

This paper is organized as follows: section 2 describes brief review of progressive visual cryptography based schemes and section 3 presents comments about Young-Chang and Zen-Yu Quan schemes. However their design would not disclose any secret information on shares if L is distributed uniformly, but on some critical chosen value of L between 1 to n, scheme caused severe security problem. We propose a chaotic sequence based PVC technique that uses 1-D chaotic map. A detailed description of the proposed algorithm is given in Section 4. Experimental results showcasing performance and security of the proposed algorithm are presented in Section 5.comparison with existing PVC based schemes are presented in section 6. Some concluding remarks are given in Section 7.

2. Review of Progressive Visual Cryptography

In this section, we briefly review the related researches in Progressive visual cryptography.

2.1 Fang's Friendly Progressive Visual Secret Sharing Scheme

Fang suggested a scheme to progressively share a halftone secret image [9]. Each secret pixel in the halftone secret image is expanded into a four-pixel block. In the decoding process, the halftone secret image can be recovered progressively by stacking the shares of different quantities. Unfortunately, this scheme suffers from the pixel-expansion problem, i.e., the sizes of the generated shares and the recovered halftone secret image increase four-fold, in other words, their size are four times as large as the original secret image.

Fang's tried to solve the problem of presence of all or nothing by progressive recovery but still it suffers from the same problem of pixel expansion which is innate drawback of traditional visual cryptography.

2.2 Progressive Visual Cryptography with Unexpanded Shares

In 2011 Young-Chang Hou and Zen-Yu Quan [7] have proposed a new scheme of progressive VC to produce pixel unexpanded shares. By stacking few pieces of shares Young's scheme gives little sketch about the original secret, but more details can be revealed if more shares are stacked and contrast will also get better.

In the method suggested by the author, encoding process will not leak out any secret information on any share. The design guarantees that the black pixels of secret image are fully restored and the contrast increases gradually as more shares are stacked and thus providing better contrast. As the block is not divided into any sub pixels in the share therefore each block contain single pixel. Thus the size of the share and secret image remains the same. Procedure of the scheme is explained in section 3.

3. Critical Analysis of Hou et al. [7] PVSS scheme

The primary issue of a VSS scheme is to safeguard the security. If during encoding process on the shares some information gets reveal then scheme losses all its credential. Prime objective behind designing any algorithm is to ensure that generated shares are not leaking sketch of original secret. As appears from Hou et.al [7], their suggested scheme gives no clue to the content of the secret image on the shares. However, realistically things are not so straight forward. Random numbers play a key-role in PVC, since they are used, to select a row from the enciphering matrices. It seems very correct that if we always choose a different number for all the pixels then shares are completely noisy in nature. Real picture depends on how you have selected a random value in the range 1 to n. Now if the range is not evenly distributed for the selection of row vector then scheme fails.

The generation of random numbers is obtained by using Pseudo Random Number Generators (PNGs). PNGs are deterministic periodic finite state machines whose aim is to emulate, within the period, the random behavior of a truly random source of numbers by using seed value. This can be predicted by post time series. From a theoretical point of view, due to their deterministic nature, PRNGs are potentially predictable by observing their generated sequence. It is worth noting that a given generator, even if belonging to a class of secure family of PNGs, can generate short periodic (and unsecure) sequences for several values of the initial seed and always has a chance of generating non uniformly distributed sequences.

So, let's think the situation where it generates all number in the range but fails to generate a single number, or, it generates a particular number fairly less compare to other generated numbers in the range. In these entire cases, scheme reveals sketch of original secret to that particular shares even during encoding and cannot be considered safe. To demonstrate, a few set of experiments were conducted and result shows that importance of selecting parameters during implementation of scheme. For experimental results, we have taken an image of (200*200) pixels as shown in Figure 1 and considered total four shares. This means, the range of random variable varies between 1to 4.

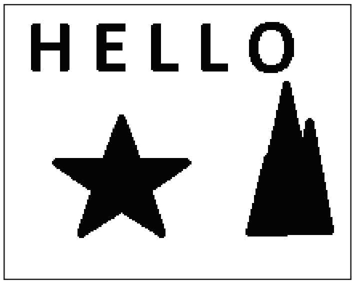

Figure 1. Test Image

We have taken seven different test cases as follows:

1. For each pixel, random number is selected as L=1 , we have found that 2nd, 3rd and 4th share completely reveals the information as shown in Figure 2.

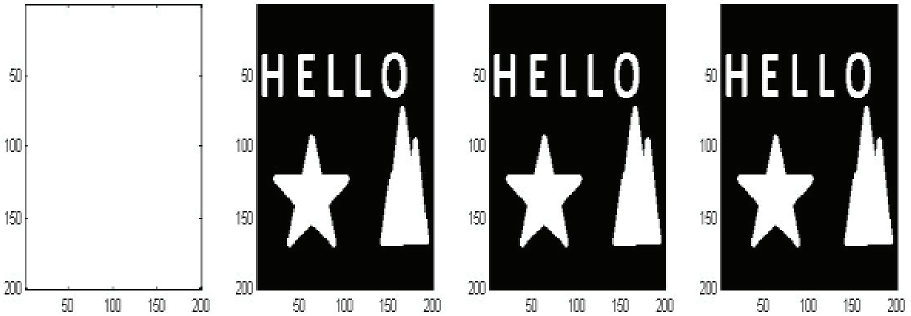

Figure 2. Generated shares for case 1

2. For each pixel, random number is selected as L=1or L=2 only; we have found that 3rd and 4th share completely reveals the information as shown in Figure 3.

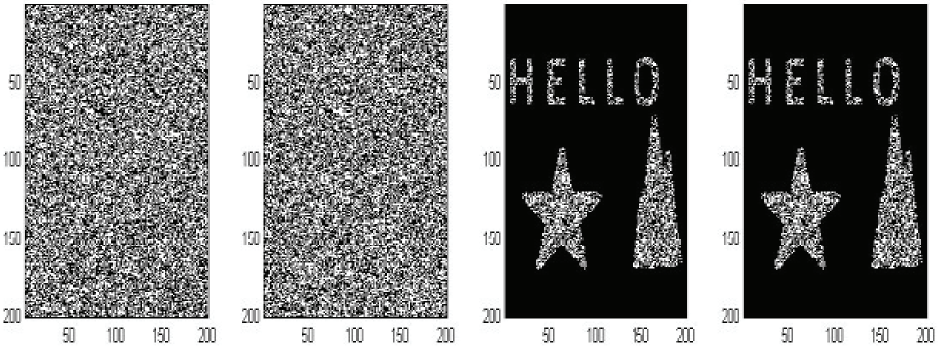

Figure 3. Generated shares for case 2

3. For each pixel, random number is selected as L=1 or 2 or 3 only; we have found that 4th share completely reveals the information as shown in Figure 4.

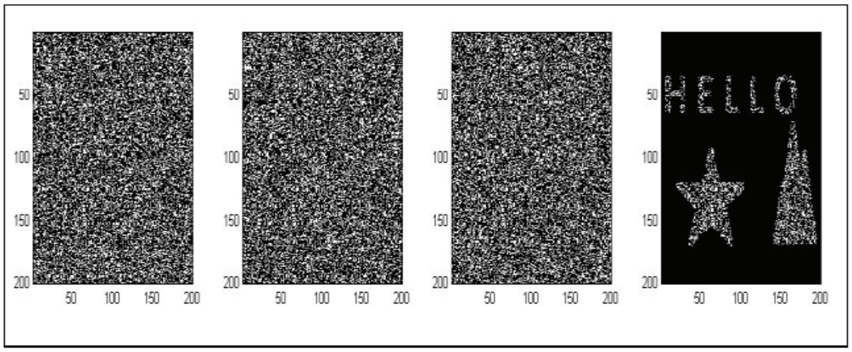

Figure 4. Generated shares for case 3

4. For each pixel, random number is selected within the range of 1 to 4, but with minimum value of L=2 or 3; we have found that 2nd, and 3rd share almost reveals the information as shown in Figure 5.

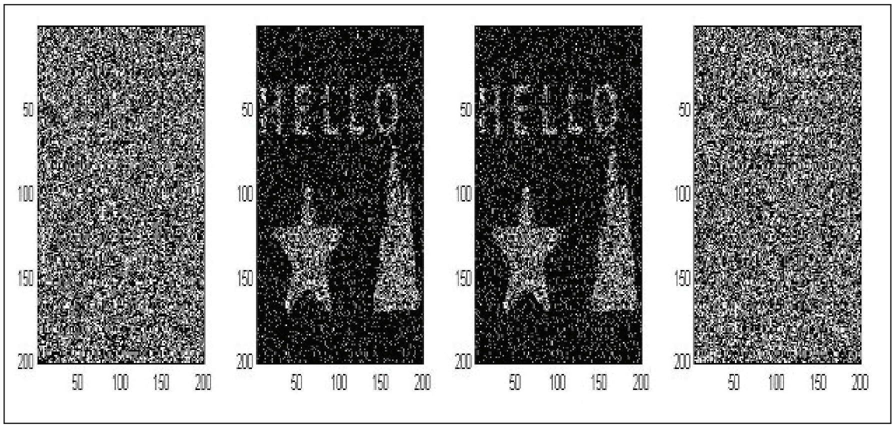

Figure 5. Generated shares for case4

5. For each pixel, random number is selected within the range of 1 to 4, but with minimum value of L=2 or 3 or 4; we have found that 2nd, 3rd and 4th share reveals the information as shown in Figure 6.

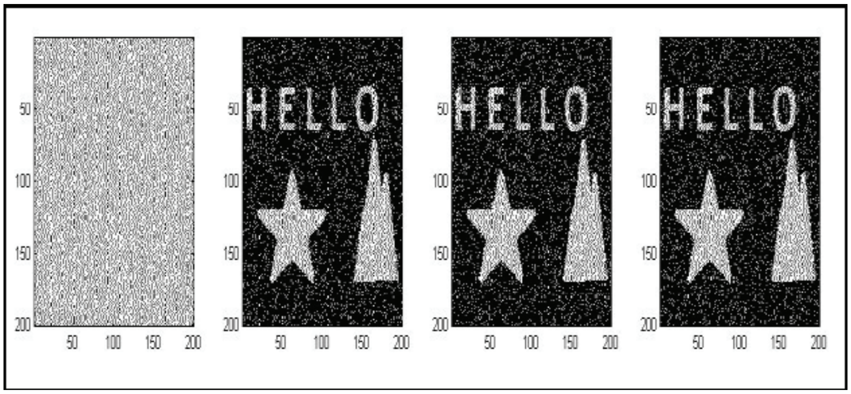

Figure 6. Generated shares for case5

6. For each pixel, random number is selected within the range of 1 to 4, but with minimum value of L=3 or 4;we have found that 3rd and 4th share reveals the information as shown in Figure 7.

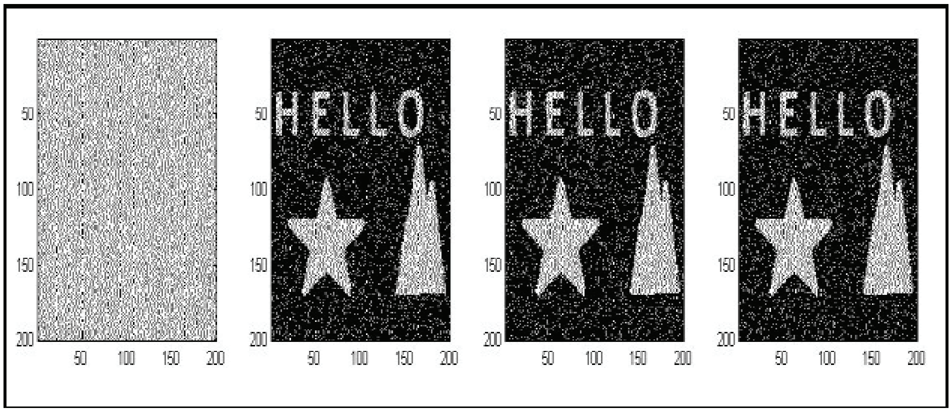

Figure 7. Generated shares for case6

7. For each pixel, random number is selected within the range of 1 to 4, but with minimum value of L=4; we have found that 4th share reveals the information as shown in Figure 8.

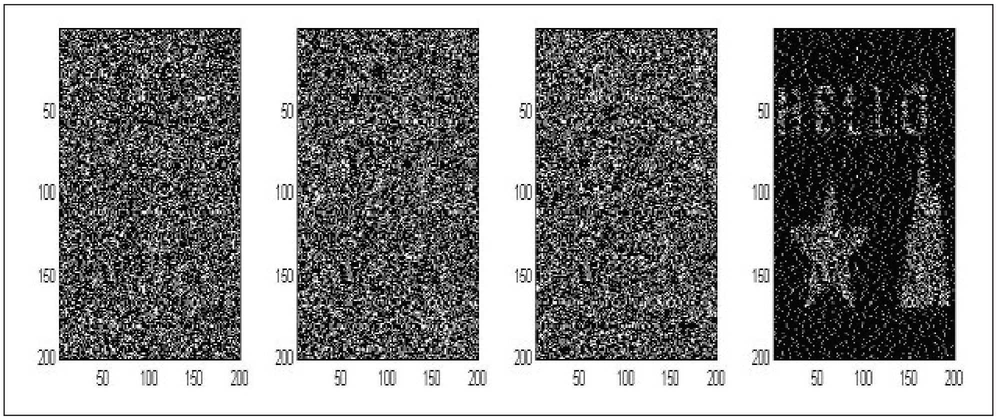

Figure 8. Generated shares for case7

It is found that cryptosystem proposed by Young et al. has a major weakness and can reveal the information in many cases. To overcome this problem the shares should be permuted properly. For making selection of L as true random, we cannot rely on common method of generating random number. So our aim is to derive nonlinear behavior from chaotic maps which in turn generates sequences that covers all the range with proper distribution and ends the chance of leaking secret in shares during encoding.

4. Proposed Algorithm

The PVC scheme proposed in this article encodes a secret image using chaotic map based random number generator. This helps imperceptibility since the significant part of the secret are not leaked during encoding process. The general assumption of a binary message results in versatility of the proposed algorithm since the message can be a text file, an image, audio, video, or any other digital content, as long as it is represented as a stream of bits. Huffman coding may be applied to the higher capacity secret message for providing compression. In the following subsections, we present the proposed algorithm in more detail. A pseudo-code of the algorithm is given here under.

Xgingenerator function uses Logistic map and local stability (Lyapunov Characteristic Exponent) of it depends on state f'(X) = r (1-2X); where r ranges from 0 to 4. We considered 10 percent noise level. One can increase or decrease noise level simply by changing it value during implementation of algorithm. This noise is observational noise. For inducing system noise, we should add the noise inside of the loop. To share a white pixel of the input image, scheme choose a xgin value generated from Xgingenerator and distribute the values of the xginth row vector of C^0 to every share, which means that the

Algorithm

Input: A $W \times H$ halftone secret image P where $P(i, j) \in P$

Output: n shares S^m, where $m = 1, 2, ..., n$ from a secret image

Process:

$$C^0 = \begin{bmatrix} 1 & 1 & \cdots & \cdots & 1 \\ 0 & 0 & \cdots & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & \cdots & 0 \end{bmatrix}_{n\times n} \qquad C^1 = \begin{bmatrix} 1 & 0 & \cdots & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & 0 & \ddots & \vdots & \vdots \\ \vdots & \cdots & \cdots & \ddots & \vdots \\ 0 & \cdots & \cdots & 0 & 1 \end{bmatrix}_{n\times n}$$

Figure 9. Sharing matrices for share generation

```
1) Generate sharing matrices $C^0$ and $C^1$ of the given form shown in Figure 9 for encoding secret message. Size of matrices is taken as $N^*N$ for both matrices.
2) For each pixel $P(i, j)$, $1 \le i \le W$, $1 \le j \le H$
        2.1) Generate a value xgin using logistic map as described in section 2.1.1
        2.1.1) Function for generation of chaotic map based xgin using logistic map
                Xgingenerator ()
                {
                        Initialize $xlog = .1$, $Noislev = 0.1$, $N = 1000$;  //Noiselev and N can be varied
                        for k = 2, 3, … $N$
                                $Alog = 4$;
                                $Xlog(k, 1) = Alog*xlog(k-1, 1) * (1- xlog(k-1, 1))$;
                        end;
                        $Xlognoise = xlog/std(xlog) + normrnd(0, Noislev, N, 1)$;
                        $b = scaledata(xlognoise, 1, K)$; //$k$ depends on number of shares
                        $c = floor(b)$;
                        $ind = round(1+(N-1) * rand(1))$;
                        $xgin = c(ind)$;
                        $return(xgin)$;
                }
3) For $m = 1, 2, ...,$ and $n$
                3.1) If the pixel $P(i, j) = 0$ (white), the pixel value $S^m(i, j) = C^0(xgin, m)$
                3.2) If the pixel $P(i, j) = 1$ (black), the pixel value $S^m(i, j) = C^1(xgin, m)$
```

first value of row vector [C^0(xgin, 1)] is distributed to share1, and the second value [C^0(xgin, 2)] is distributed to share2, and so on. C^1 is applied to share a black pixel with the same sharing strategy as sharing for a white pixel.

5. Performance Analysis and Experimental Results

A concrete evaluation of the quality of a modified image can be made using similarity measures. Existing measures of similarity includes the mean squared error (MSE), the peak signal to noise ratio (PSNR), and the structural similarity (SSIM) index [10]. The MSE is the average value of the square of the difference between the two images. MSE is not necessarily a good indicator of quality to hide message in an encoded share. The PSNR is in essence the logarithm of the reciprocal of the MSE. Although recently SSIM seems to be a better measure of the quality of encoded shares, PSNR is more commonly reported. To make comparison of our algorithm with existing work possible, we report both PSNR and MSE values here. We present an evaluation of the imperceptibility of the proposed algorithm in terms of the peak signal to noise ratio (PSNR), and also calculated entropy for each shares. Entropy measures the uncertainty association with random variable in a system. In a secure system, the information entropy of the ciphered image should not provide any information about the plain image. The information entropy was calculated for each encoded shares as well as the overlapped reconstructed shares. For experimental results, we have taken an image of (200*200) pixels as shown in Figure 1 and considered six shares and number of iteration N was chosen as 2000 for generating chaotic random number using logistic map.

Share No.	MSE	PSNR	Entropy
S1 share	0.3130	53.2090	0.7085
S2 share	0.3181	53.1395	0.7064
S3 share	0.3137	53.1630	0.6951
S4 share	0.3129	53.2180	0.6970
S5 share	0.3108	53.2403	0.7170
S6 share	0.3186	53.1327	0.7050
S12 share	0.2815	53.6704	0.7780
S123 share	0.2556	54.0896	0.8211
S1234 share	0.2289	54.5693	0.8611
S12345 share	0.1900	55.3773	0.9047
S123456 share	0.1590	56.1522	0.9353

Table 1. Results of proposed algorithm

From the results, the entropy values for each share generated by the algorithm proof to be very effective. The values remain approximately close and the share images are visually unrecognizable, thus it reduces the chance of leaking sketch during the process of encoding. This makes the algorithm very efficient. The total entropy of the plain images remained constant, since there has been no pixel expansion. We also perform a comparison with some existing PVC schemes.

6. Comparison with Existing Work

There exist many articles which propose traditional and progressive visual cryptography algorithms. It should be noted that in progressive techniques encoded shares should not reveal anything as well as there should not be any pixel expansion also. Traditional schemes suffer from the problem of pixel expansion as well as usually provide a reduced quality of the recovered images. There is a trade-off between quality and security in available schemes. Thus for our comparison with existing work, we choose the algorithms of [6, 7, 9]. This selection is based on the fact that these papers introduce progressive sharing concept. We run some of the concept reported in [6, 7, 9] for comparison of the results with our proposed algorithm. Results of these tests are summarized in Table2 and clearly indicate that the algorithm proposed by this paper outperforms all these three algorithms in terms of security preservation and pixel expansion problem. Further Table3 indicates the value of entropy of each shares generated by proposed scheme as well by Hou et al.[7] for case eg.3 as indicated earlier in this paper. Results as shown in Graph.1 proof that sharp change in entropy value between the shares of Hou et al. scheme although it remains approximately similar in all the shares by proposed scheme. Sharp fall in graph is due to leakage of sketch in case3 for the share number four, five and six. This validates that chance of leaking secret during encoding is not possible because of high degree of randomness suggested by the proposed scheme using chaotic map. PSNR and MSE comparison between the schemes is presented in Table4. Results as shown in Graph.2 indicate a better reconstructed image for proposed scheme in terms of contrast and no sketch leakage in shares.

Scheme	Kernel technique	Content of shares	Pixel Expansion	Visually Progressive	Leakage of secret
Hou and Quan [7]	PVC	leakage of Structure	NO	Yes	Yes
W.P. Fang [9]	PVC	Meaningful	YES	Yes	Yes
Fang and Lin [6]	PVC	Noise –like	YES	Yes	Yes
Proposed Scheme	PVC	Noise Like	NO	Yes	No

Table 2. Comparison with well-known PVC schemes

Progressive Scheme	Entropy					
	Share1	Share2	Share3	Share4	Share5	Share6
PVC Hou et al.[7] eg. Case3	0.9181	0.9215	0.9210	0.8441	0.8241	0.8241
Proposed Scheme	0.7085	0.7064	0.7051	0.7170	0.7170	0.7050

Table 3. Results of Entropy Values in the shares of compared schemes

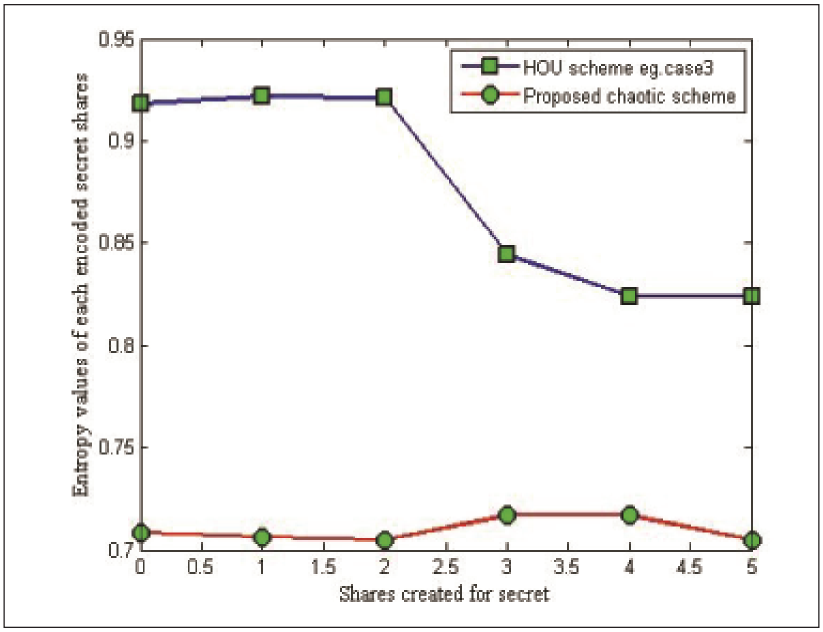

Figure 1. A graph of Entropy values comparison shown in Table 3

7. Conclusion

A robust progressive secret sharing technique, based on chaotic map is proposed in this paper. The irregular outputs of the logistic map are used to scatter in a random-like manner, a secret digital message for sharing. The use of chaotic map based random number generation with increased number of iteration guarantees security of the information in generated noise like shares. In particular, it is shown that the proposed algorithm has good imperceptibility. Finally, in comparison with some existing PVC schemes, the algorithm proposed is shown to have superior performance. It is well known that the confusion in the encryption process is ultimately related to the security i.e. more confusion leads to more security. Hence it can be said that by using the proposed algorithm one can transmit the secret message with more security as compared to the existing

Scheme	Share no.	MSE	PSNR
PVC Hou Scheme [eg. Case 3]	Share1	0.3983	52.1622
	Share2	0.3961	52.1868
	Share3	0.3967	52.1805
	Share4	0.4606	51.5356
	Share5	0.4606	51.5356
	Share6	0.4606	51.5356
	Recovered Secret	0.2702	53.8475
Proposed Scheme	Share1	0.3130	53.2090
	Share2	0.3181	53.1395
	Share3	0.3137	53.1630
	Share4	0.3129	53.2180
	Share5	0.3108	53.2403
	Share6	0.3186	53.1327
	Recovered Secret	0.1590	56.1522

Table 4. PSNR and MSE values of compared schemes

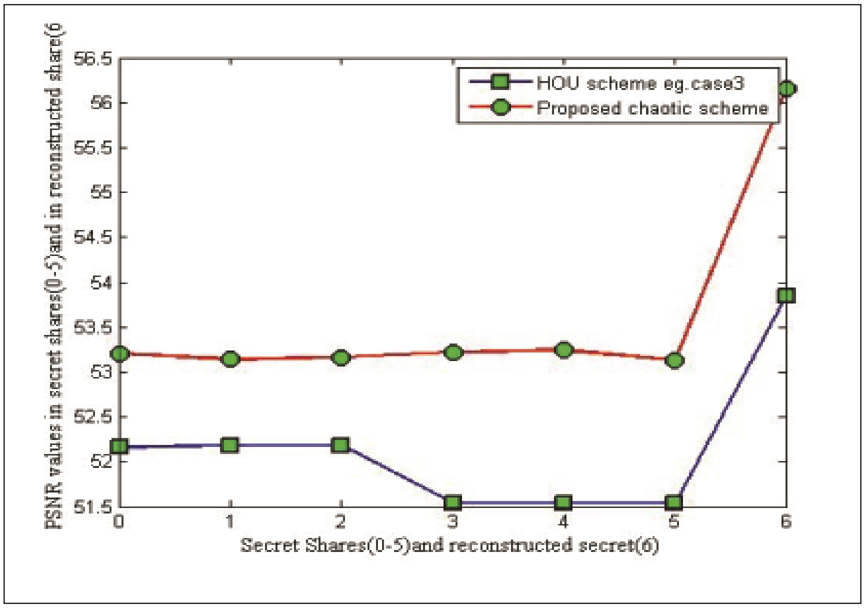

Figure 2. A graph of PSNR comparison shown in Table 4

PVC. Besides the robust security and production of the shares having same size as its corresponding secret message, the presented algorithm also possesses the better recovered secret image as compared to traditional approaches.

In summary, we have extended the idea of progressive digital secret sharing further by introducing logistic chaotic maps in the algorithm for generating leak proof shares. We have used one prototype of chaotic map however; it can be easily extended to any other chaotic maps.

References

[1] Naor, M., Shamir, A. (1995) Visual cryptography, *In* : Proceedings Adv. Cryptol. *EUROCRYPT*, 950. 1–12.

[2] Eisen, P. A., Stinson, D. R. (2002). Threshold visual cryptography schemes with specified whiteness levels of reconstructed pixels, Des., *Codes Crypt*., 25 (1), 15–61.

[3] Fang, W. P. (2007). Multilayer progressive secret image sharing *In*: Proceedings 7*th* WSEAS, 112–116.

[4] Jin, D., Yan, W. Q., Kankanhalli, M. S. (2005). Progressive color visual cryptography, *J. Electron. Imag.*, 14 (3) 1–13.

[5] Petrauskien, Vilma., Survila, Arvydas., Fedaravicius, Algimantas., Ragulskis, Minvydas. (2014). Dynamic visual cryptography for optical assessment of chaotic oscillations , Elsevier, *Optics & Laser Technology* 57, 129–135.

[6] Fang, W. P., Lin, J. C. (2006). Progressive viewing and sharing of sensitive images, *Patt. Recog. Image Anal*., 16 (4) 638–642.

[7] Hou, Young-Chang., Zen-Yu Quan. (2011). Progressive Visual Cryptography with Unexpanded Shares , *IEEE Transactions On Circuits And Systems For Video Technology*, 21 (11) C. C. Thien., J. C. Lin, Secret image sharing, *Comput. Graphics*, 26 (5) 765–770, 2002.

[8] Fang, W. P. (2008). Friendly progressive visual secret sharing, *Pattern Recognition*, 41 (4) 1410–1414.

[9] Wang, Z., Bovik, A., Sheikh, H., Simoncelli, E. (2004). Image quality assessment: from error visibility to structural similarity, *IEEE Transaction on Image Processing* 13 (4), 600–12.