Journal of Engineering and Applied Sciences 14 (23): 8600-8608, 2019
ISSN: 1816-949X

Halftone Visual Crytography Schmeme for Color Image using Dynamic Codebook and Chaotic Map

Rasha Subhi Hameed and Abdul-Wahab Sami Ibrahim
Department of Computer Science, Collage of Education, Mustansiriyah University, Baghdad, Iraq
techer.prg83@gmail.com

Abstract: Halftone visual cryptography is method for encoding secret image to generated secure meaningful shares images. In this study, halftone visual cryptography scheme using dynamic codebook and chaotic maps technique is proposed for natural color image by using dynamic codebook technique the proposed method can be retrieve color secret image with perfect size and contrast as well as proposed a novel technique to distributed secret image pixels into covers image in randomly and homogenous manner based on 2 chaotic maps (logistic and Chevbyshev 1D maps). This scheme gives to the dealer absolute control to check authentication each block in the income shares and flexibility in the management share images. The experimental results, performance MSE , PSNR ,UQI , SSIM and NCC metrics shown improvement in visual quality for shares image and ideal results for recovered color secret image.

Key words: Halftone Visual Cryptography (HVC), Error Diffusion (ED), image quality metrics, logistic 1D map, Chevbyshev 1D maps, visual quality

INTRODUCTION

Information security play a very important role in internet computing environment. Multimedia data like images, video, audio etc. are widely used and shared over internet. These data are very sensitive, therefore, security issues should be taken into consideration. One of the strongest encryption technology is the Visual Cryptography Scheme (VCS) that ensuring security of the sharing images and information without using encryption and decryption keys. Noar and Shamir (1995) first proposed "Visual Cryptography Scheme (VCS)" to encode 1 binary secret image and split it into n several parts called shares. The n shares are usually printed in transparencies. Each of the n shares will be distributed to n participants. When all the n shares are stacked, the original image is visible by the human eye, no need to any complex computation. Any (n-1) shares will retrieval no information about the original. Although, this scheme represents new direction in digital image cryptography but it has some weak points such as the problem of static codebook like large pixel expansion, low contrast, cross-interference and the random share is raised suspension from attacks side. For overcome these problem (Mishra and Biswaranjan, 2015) introduced Extended Visual Cryptography Scheme (EVCS) to generation meaningful share images instead of random shares by embedding the secret pixels into cover images but this scheme still have low visual quality problem. For this reasons Liu and Wu (2011) proposed Embedded Extended Visual Cryptography (EEVC) based on dithering halftone techniques to embedded SIP (Secret Information Pixels) into cover image to produce meaningful share images. In general, Halftone Visual Cryptography scheme (HVCs) used to embed a secret image pixels into meaningful shares with higher visual quality. HVCs have number of problems like double the size and low contrast of the secret image returned and cross-interference problems and this scheme unable to handle the color of the images with high resolution as efficiently form and difficult to manage shares images (Chen, 2013).

The first proposed HVC scheme are (Zhou *et al*., 2006) based on dithering halftone techniques and conventional VC scheme to encode binary image into halftone cover images and by using "void and clustering algorithm" to determine location of SIP (Secret Information Pixels) but this algorithm need more computation and time. To overcome this problem, Wang *et al.* (2009) introduced enhancement HVCs by using error diffusion halftone technique which characteristic more simple and produce better visual quality shares furthermore (Alex and Anbarasi, 2011) used various error diffusion techniques such as (classical fixed, edge enhancement, green noise and block error diffusion)

Corresponding Author: Rasha Subhi Hameed, Department of Computer Science, Collage of Education, Mustansiriyah University, Baghdad, Iraq, techer.prg83@gmail.com

to enhancement halftone shares quality but the visual quality of these shares still needs more enhancement. Hodeish and Humbe (2018) are proposed Optimal Halftone Visual Cryptography (OHVC) scheme to eliminate the explicit of the demand of codebook and produced semi-random shares images via. encoding only black secret pixel while leaving the white secret pixels without change. But this scheme deal only with binary secret image and still contrast need to improved. Pahuja and Kasana (2017) are suggest development Floyd-Steinberg's error diffusion for gray scale and color images based on (2, 2-HVC) and decomposed color technique, in this scheme, the codebook design required large memory space and the color intensity of recovered secret is change. From the above summary, the proposed method for color image by using dynamic codebook can be overcome all problem that are reviewed above and proposed a novel technique by using two kind of chaotic maps logistic and Chevbyshev 1d maps) to distributed SIP in cover images in randomly location for enhancement security level for the proposed method.

MATERIALS AND METHODS

Proposed halftone visual cryptography scheme for encryption and embedding color image using dynamic codebook and chaotic maps.

In this method, an input RGB secret image is encrypted into six meaningful shares. To recovered the secret image by stacking in order k shares, any (k-1) share reveal no any information about the secret image. The proposed method consist from five steps as following.

Preprocessing step: The secret image and 6 cover images passed through preprocess phase, the direction of this step shown in algorithm 1.

Algorithm 1; Preprocess step:

for color secret and cover image
Input:
S//color secret image
C//color cover image
Output:
HSR, HSG, HSB//halftone secret image
HC//halftone cover image
Begin
Step1: Apply error diffusion on S and C to generation HS and HC
Step2: Split the HS image into three Color bands HSR, HSG, HSB
Step3: Apply Histogram on each HSR, HSG, HSB separately and respectively
End algorithm

Algorithm 1 applying Burkes error diffusion halftone technique on secret and cover images by using Burkes

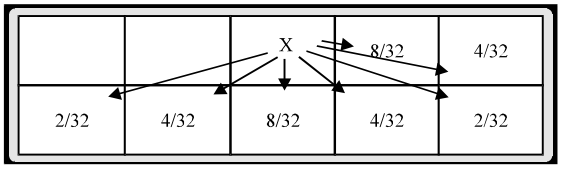

Fig. 1: Burkes E-D coefficients matrix

coefficients matrix (Pahuja and Kasana, 2017) as show in Fig. 1. Where, x represent current pixel process to diffusion the error to 7 of neighbors. Burkes ED results better visual quality.

Encoding color secret image step: in this phase, encoding Halftone Secret image (HS) by using novel technique called Dynamic Code Book (DCB) to generation encode secret pixels, the main idea of this technique is given for each secret pixel an unique binary code. The direction of this step illustrated in algorithm 2.

Algorithm 2; Encoding step by using dynamic codebook:

Input:
HSR, HSG, HSB//halftone secret image
Output: 6 random shares
Begin:
Step1: Give for each pixel in HSR (order, binary code (BIN))
Step2: BIN = 12 bits (the number 1's bits must be equal number of 0's Bits)
Step3: Mask1[4, 4] = BIN
Mask2[4, 4] = complement (BIN), the 4 row indicated for flags
Step4: If Mask1 [4,4]• Mask2 [4,4] = = 0000000000000
Then place Mask1 to first location for share1 and place Mask2 to first location in share2
Step 5:Repeate step 1-4 for encoding HSG, HSB
End algorithm

Figure 2 illustrated dynamic codebook technique and shown the way of distributed binary code in mask cell when the size of mask cell is (4 row, 4 column).

Generate random location for SIP by using logistic and Chevbyshev chaotic maps: After produce 6 random share by using dynamic codebook in this step, determine location for each SIP in random shares this position must be homogenous and randomly as possible this can done by two sub step:

- First step: create period table as shown in algorithm 3
- Second step: generate random location as shown in algorithm 4

In this step, the proposed method using two chaotic system: logistic 1d maps: logistic mapping chaotic sequence is simplest nonlinear model a chaotic map that occurs in real systems. Logistic 1D maps can show chaotic behavior by Eq. 1:

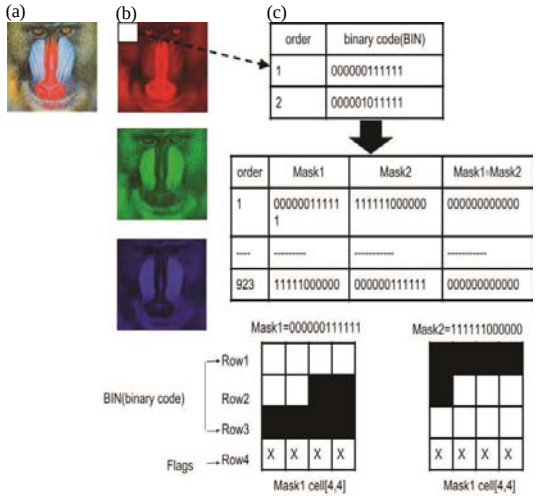

Fig. 2: Encoding step by using dynamic codebook: a) Input secret image; b) HSR, HSG, HSB (histogram halftone secret image for RGB color bands), respectively and c) Dynamic codebook mechanism

$$X\_(n+1) = \mu X\_n(1 - X\_n) \quad (1)$$

where, X• [0, 1], μ represent bifurcation parameters, if we change the value of μ the logistic map behaviour is changes drastically. The logistic maps became in chaotic stats when 3.5699• μ<4 sequence of the logistic function has the features of simple shapes and sensitivity to initial conditions (Xiao *et al*., 2018).

Chevbyshev mapping: Chaotic sequence which is one of most used security mechanisms in authentication methods because it has semi-group property. The Chevbyshev polynomial presented in three definitions of as following (Quan *et al*., 2018).

Definition 1: The Chevbyshev polynomial in degree n is determined as:

$$Tn(x) = \cos(n \times \arccos(x))$$

where, n is integer number, x• [-1 , 1].

Definition 2: Semi-group features for Chevbyshev can achieved as:

$$Trs(x) = Tr(Ts(x)) = Ts(Tr(x))$$

Definition 3: The Chevbyshev polynomial in n degree, present:

$$(x, Tx(x))$$

it is infeasible in computation to determine the polynomial order n.

Algorithm 3; Create period table:

```
Input: From//initial value for period
       To//ending value for period
       xStep//Decrement value for each step
Output: Table (no, From,To)
Begin:
 Step1: From = 1: xStep = 1/32
        To = From-xStep
        Table Add(1, From, To)
        From = To
 Step2: For i = 2-32
        To = From-xStep
        Table Add (i, From, To)
        From = To
 End algorithm
```

Algorithm 4; Generate random location for SIP:

```
Input: Fixedblock //number of "0"
       xwidth//width of input image
       xkey//integer number
       nrow//number of rows in periods table which equal 32
       x00,x0//initial value for logistic and Chevbyshev function
       xBlock1 and 2//Boolean array
Output: set of random location xkey
Begin: Step1:create Eprom
Step 2:
Step 2-1: For iL = 0 to xwidth
          Logistic value = r (x00*(1-x00))
          swap (x00, Logistic value)
          loct = 0
          For n = 0 to nrow
          {
         If ( Logistic value > = index[n] & Logistic value <index[n])
         then loct = n
         }//*end For
Step 2-2: while (true) {
          Chevbyshev value = cos (k (cos-1 (x0)))
swap (x0, Chevbyshev value)
xBlock2 = xBlock2+D2B(CHEBYSHEV value, Fixedblock)
if (xBlock1.Length >32+1) then end loop}//*end
while
Step 2-3: Determine two equal parts in Eprom each part represent 32
locations and assigned the pointer i for part1 and pointer j for part
          For i = 0 to Eprom size/2
          {
          if (xBlock1[i] != xBlock2[i]) then swap
(Eprom[i], Eprom[j])
          }//*end For
Step2-4: If (k • (xwidth xwidth)-1)
{
xkey = Eprom[loct]
If (xkey == -1) Then fined nearest value to Eprom[loct] != -1 and assigned
to xkey and replaced value of this location in Eprom by -1 Else Eprom
[loct] = -1
End if
Else xkey = Eprom [loct]
k = k+1
Eprom[loct] = -1
}//*End If
}//*End For
Step3: Repeated step 2 until get all location that neede to embedded all
Secret pixels
End algorithm
```

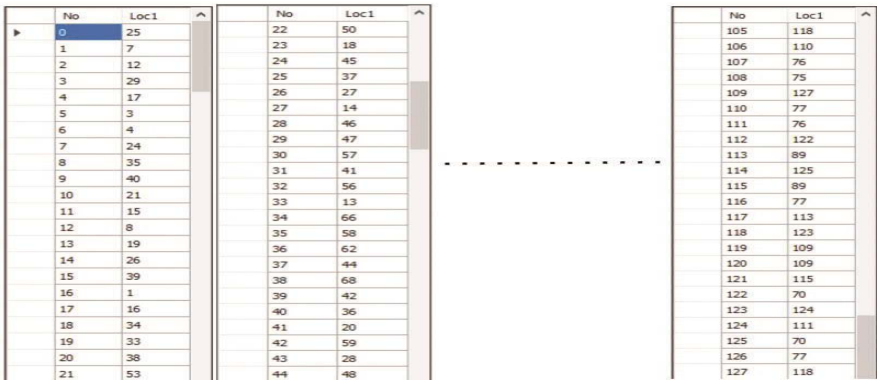

Fig. 3: Random location by using logistic and Chevbyshev chaotic maps

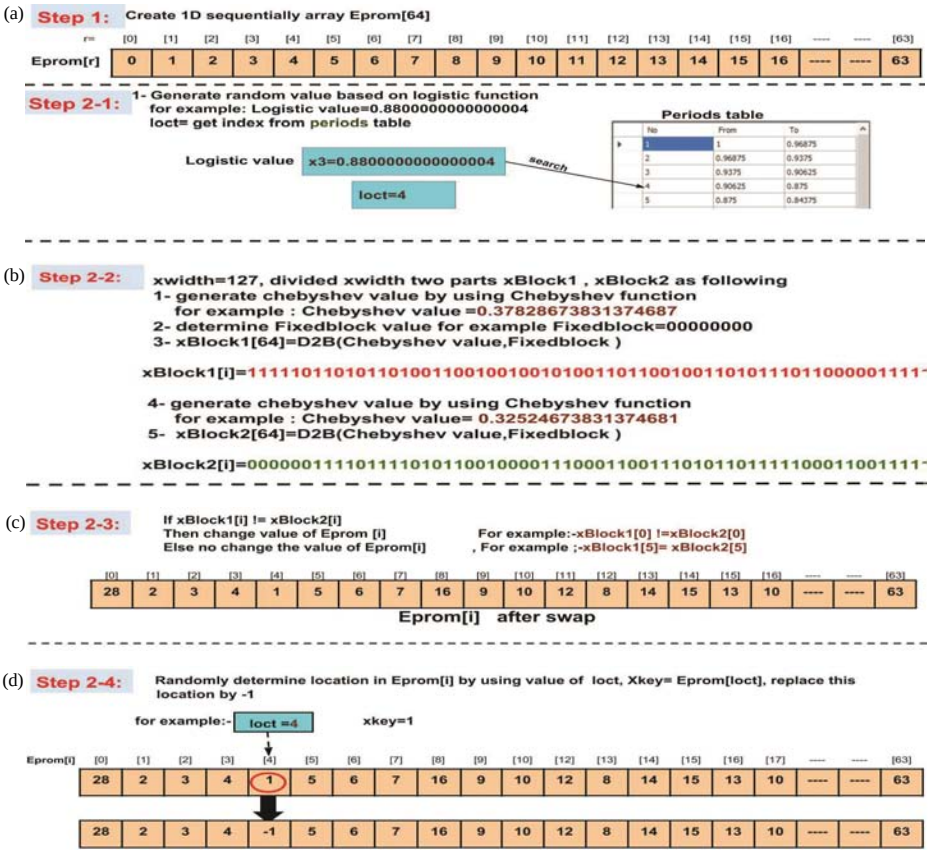

Fig. 4: a-d) Examples for generate random location by using logistic and Chevbyshev chaotic maps

Figure 3 shown, the result of algorithm 5 which is represent random location by using logistic and Chevbyshev chaotic maps and Fig. 4 shown, example for each step in algorithm 5.

Embedding SIP into six natural color cover images step: In this step using new techniques to embedded the SIP (Secret Information Pixels) into cover images to generate meaningful share images by using flags techniques. The direction for this step illustrated in algorithm 5.

Algorithm 5; Generate meaningful share images by using new embedding technique:

Input: random share1
HC//Halftone Cover image

m, n//index of halftone cell
x, y//index of mask cell
Output: Meaningful share image
Begin:
Step1: z = 0
Divided HC to q[m, n] cell and divided random share to MC[x, y] cell
Step2: For m = 1-4
For n = 1-4 {
x = I, y = j
If MC[x,y] = 1 Then z = q[m, n], q¯[m, n] = q[m, n],q¯[4, 1] = q¯[4, 2]
End if
Else If (MC[x, y] = 1 & q[m, n] = z) Then q¯[m, n] = q[m, n]
End if
Else If (MC[x, y] = 1 & q[m, n] = z)
Then q¯[m, n] = z End if
Else If (MC[x, y] = 0 & q[m, n] = z)
Then (q¯[m, n] = q[m, n]-1) OR (q¯[m, n] = q[m, n]+1)
End if
Else If (MC[x,y]=0 &q[m,n] • z) Then q¯ [m, n] = q[m, n] End if
}//*End all for
Step3: Repeated step 1 and 2 to embedded all Mask cells MC[x, y] into all halftone cell (q¯[m, n]) in HCI to generate random share
End algorithm

Recover color secret image step: When dealer want to retrieve the color secret image, he must be first stack in order all k shares then the secret image recover by using human eye only. Any (k-1) shares cannot recover any information about the original secret image. The direction of this step illustrated in algorithm 6.

Algorithm 6; Recovering step based XOR operation:
Input:{Share 1, Share 2},{Share 3, Share 4},{Share 5, Share 6}
Output: HSI//Halftone secret image
Begin:
Step1: Determined first q¯cell in Share 1 and Extract value of (z)//*z is variable dedicated to q¯cell
Step2: If (q¯[4, 1] = q¯[4, 2])&(q¯[m, n] = z) Then q¯m, n] = 1
Else If(q¯[4, 1] = q¯[4, 2])&(q¯[m, n]• z)Then q¯[m, n] = 0
}//*end If
}//*End For
Step 3: Repeated Step 1, Step 2 for Share 2
Step 4: If binary code for q¯cell in Share 1 • binary code for q¯cell in Share 2 = 000000000000. Then go to Step 5
Else, go to step 1
End if
Step 5: Get (No) from dynamic codebook where
q¯ = Bin
Step 6:Repeated Step 1-5 to recover {HSI1, HSI2, HSI3}
Step 7: HSI = HSI1• HSI2• HSI3
End algorithm

RESULTS AND DISCUSSION

Two experiments are implemented in the proposed method. By using Lena. BMP, Babbon.JPG: represents secret images with size 128×128 in RGB color space and "Peppers, Mount, Flow, Female, House, Flower vase.JPG" as cover image with size 255×255 in RGB color space as shown in Fig. 5, represents result of pre-processes step for secret image and Fig. 6 represents result of pre-processes step for cover image.

Figure 7 shown, the generated random location by using logistic and Chevbyshev chaotic system when value of Fixedblock = 4. Figure 8 shown, the generated random location by using Logistic and Chevbyshev chaotic system when value of Fixedblock = 8. Figure 9 shown, the generated random location by using logistic and Chevbyshev chaotic system when value of Fixedblock = 10.

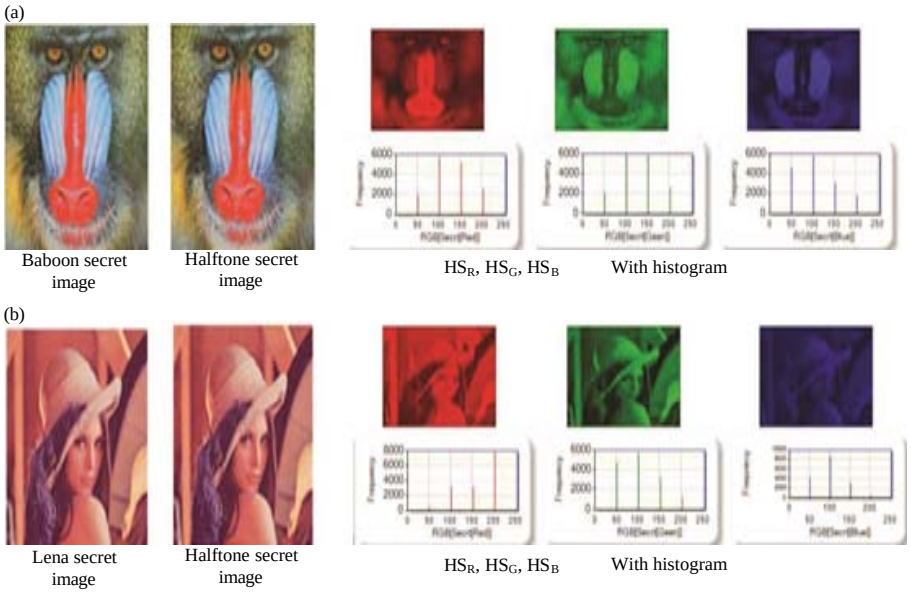

Fig. 5: Simulate result of preprocess step for both experiments: a) First experiment with Baboon.JPG secret image and b) Second experiment with Lena.PMB

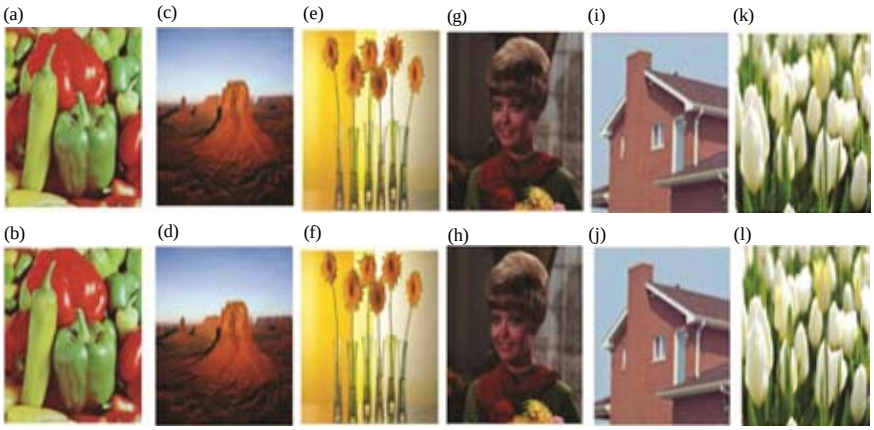

Fig. 6: Simulate result of preprocess step for cover images: a) Pepper cover 1 image; b) Halftone cover 1 image; c) Mount cover 2 image; d) Halftone cover 2 image; e) Flow cover 3 image; f) Halftone cover 3 image; g) Female cover 4 image; h) Halftone cover 4 image; i) House cover 5 image; j) Halftone cover 5 image; k) Flowers cover 6 image and l) Halftone cover 6 image

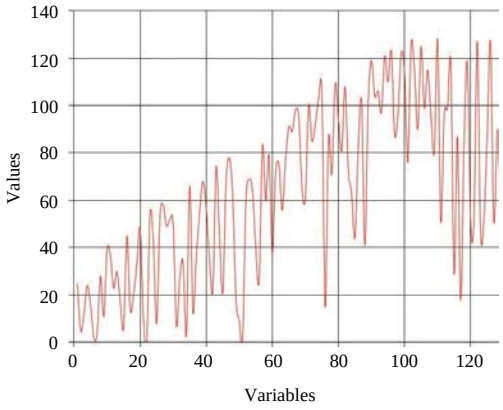

Fig. 7: Generate random location when Fixedblock = 4

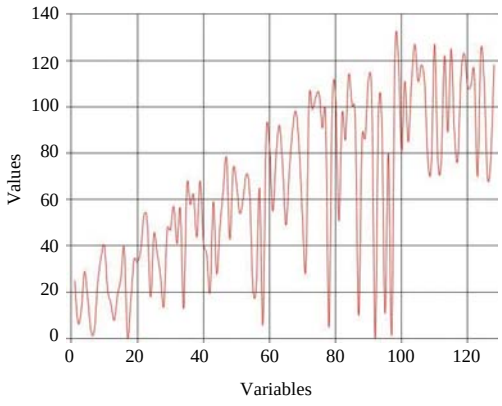

Fig. 8: Generate random location when Fixedblock = 8

From Fig. 7-9, in our proposed method we will depend on values of Fixedblock = 8, the result

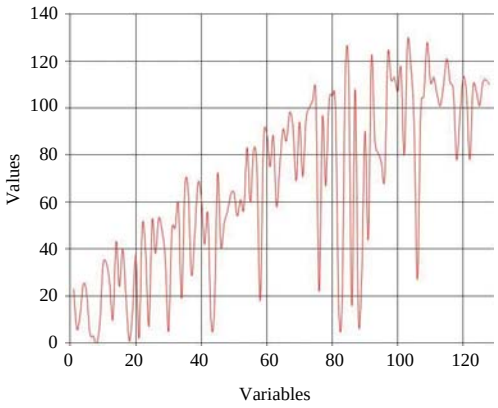

Fig. 9: Generate random location when Fixedblock = 10

of embedding technique which is represents generated six meaningful share images as illustrate in Fig. 10.

The result of recovering technique to recover the halftone secret image by using only human vision system as illustrated in Fig. 11 for both experiments.

MSE, PSNR, UQI, SSIM and NCC are used to evaluation result of proposed method. Mean Squared Error (MSE) is one of image quality index. Is measure the different between input images and the output image when the value of MSE became smaller that mean the image have good quality. MSE computed as following (Kumar and Chandramathi, 2016):

$$MSE = \frac{1}{M.N}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\left[I(i,j)-k(i,j)\right]^2$$

Fig. 10: Generate meaningful share images: a) Cover images before embedded the SIP and b) Cover images after embedded the SIP

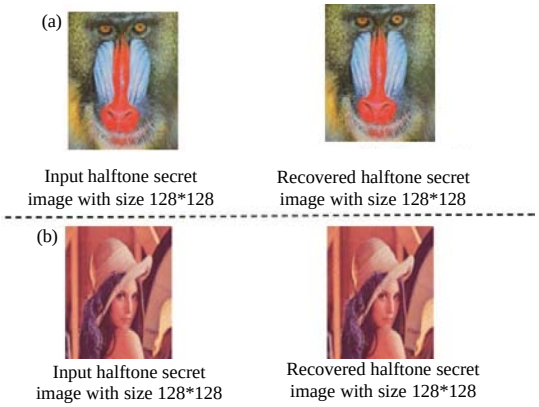

Fig. 11: Simulate result of recovering technique by using flags: a) First experiment with baboon.JPG halftone secret image and b) Second experiment with Lena.PMB halftone secret image

Peak Signal to Noise Ratio (PSNR) is ratio metrics between maximum single power to power of the mess up noise that generates distortion of image (Kumar and Chandramathi, 2016; Badal, 2017):

$$PSNR = 10\log_{10}(MAX^2 \bullet MSE)$$

Universal image Quality Index (UQI) is quality measurement method is not depend on tested images for now but it must be usable to different image processing application, the ideal value for (UQI) is between [-1, 1]. UQI can computed as following:

$$UQI = \frac{4\sigma_{xy}\overline{x}\overline{y}}{\left(\sigma_{x^2} + \sigma_{y^2}\right)\left[\overline{x}^2 + \overline{y}^2\right]}$$

Structure Similarity Index Method (SSIM) is measure used to determine the similarity ratio between two images.

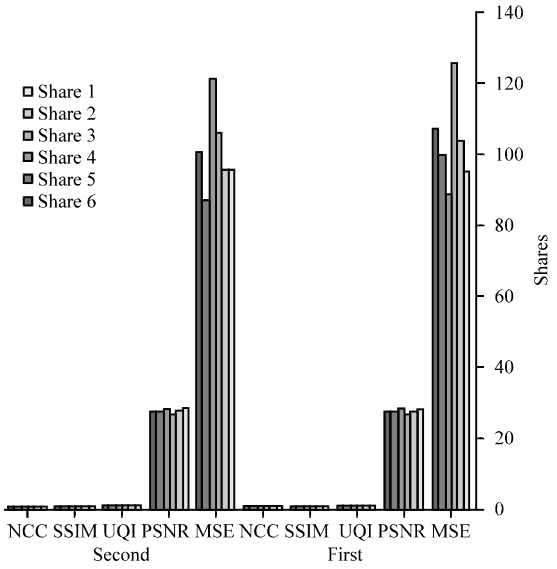

Fig. 12: Comparison between two experiments based MSE, PSNR, UQI, SSIM, NCC metrics

The SSIM is full reference measure. The ideal value for SSIM is 1. SSIM computed as following (Kumar and Chandramathi, 2016):

$$SSIM = \frac{\left(2\mu_X.\mu_Y C1\right)\left(2\sigma_{XY} + C2\right)}{\left(\mu_{X^2} + \mu_{Y^2} + C1\right)\left(\sigma_{X^2}\sigma_{Y^2} + C2\right)}$$

Normalized Cross Correlation (NCC) is one of quality image index that measure the similarity between two function the optimal value of NCC is 1. NCC computed as following (Kumar and Chandramathi, 2016):

$$NCC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} x(i,j).y(i,j)}{\sum_{i=1}^{M}\sum_{j=1}^{N}\left(x(i,j)^2\right)}$$

MSE, PSNR, UQI, SSIM and NCC values are computed between input halftone secret image and its corresponding recovered halftone secret image and between halftone cover images HC and their corresponding meaningful shares images for both as shown in Table 1 for first experiment and Table 2 for second experiment (Fig. 12).

From value of image quality metrics in Table 1 and 2 for both experiment show that the recover halftone secret image in same size, contrast, the recovered halftone secret image not suffer from cross-interference and the intensity of secret image pixels color are recovered without any change. From value of image quality metrics in Table 1 and 2 for both experiment show the visual quality of

Table 1: First experiment for proposed method

Metrics	HS	Share 1	Share 2	Share 3	Share 4	Share 5	Share 6
MSE	0.0000	95.0017	103.8580	125.7067	88.8826	100.1693	107.1466
PSNR	•	23.3535	27.9664	27.1372	28.6426	28.1235	27.8310
UQI	1.0000	0.9935	0.9947	0.9904	0.9950	0.9894	0.9924
SSIM	1.0000	0.9562	0.9409	0.8399	0.8393	0.9907	0.9960
NCC	1.0000	0.9935	0.9947	0.9904	0.9950	0.9894	0.9924

Table 2: Second experiment for proposed method

Metrics	HS	Share 1	Share 2	Share 3	Share 4	Share 5	Share 6
MSE	0.0000	95.6073	95.6073	105.9356	121.2757	87.8729	100.7575
PSNR	•	28.3259	27.8804	27.2931	28.6923	28.0980	27.8210
UQI	1.0000	0.9935	0.9946	0.9907	0.9951	0.9893	0.9924
SSIM	1.0000	0.9582	0.9418	0.8433	0.8411	0.9907	0.9960
NCC	1.0000	0.9935	0.9946	0.9907	0.9951	0.9893	0.9924

shares images is improvement and don't suffer from cross-interference which is consider bigger problem. Chart 1 in Fig. 12 shown, comparison between two experiments based on image quality metrics in Table 1 and 2.

Chart in Fig. 12 shows, the values of parameters of the image quality metrics for share images for both experiments we can note the second experiment with HS.BMP have better result more than first experiment with HS.JPG.

CONCLUSION

In this study, HVCs for color image using dynamic codebook, error diffusion and logistic and Chevbyshev chaotic 1D maps. The proposed methods eliminate the HVC scheme limitations of the static codebook that is requirement more time and memory in design we dealing with color secret image with higher resolution and the consequences of using it is pixel expansion. By using dynamic codebook and Bruker error diffusion the proposed method able to recover color secret image with optimal value based on image quality metrics and by using chaotic maps the proposed scheme have higher security level and considered novel technique to distributed SIP in perfect way without effected on visual quality of final share images and finally by using authentication shares technique given to dealer ability to accept or reject the income shares. The decryption secret image done based on XOR-Boolean operation without any complex computation.

REFERENCES

Alex, N.S. and L.J. Anbarasi, 2011. Enhanced image secret sharing via. error diffusion in halftone visual cryptography. Proceedings of the 3rd International Conference on Electronics Computer Technology Vol. 2, April 8-10, 2011, IEEE, Kanyakumari, India, ISBN:978-1-4244-8678-6, pp: 393-397.

Badal, N., 2017. Approaches of visual cryptography for gray scale and color images using error-diffusion halftoning technic. Intl. J. Comput. Sci. Inf. Technol. Secur., 7: 7-16.

Chen, W.K., 2013. Image sharing method for gray-level images. J. Syst. Softw., 86: 581-585.

Hodeish, M.E. and V.T. Humbe, 2018. An optimized halftone visual cryptography scheme using error diffusion. Multimedia Tools Appl., 77: 24937-24953.

Kumar, R.R. and S. Chandramathi, 2016. Color visual cryptography scheme for natural images using complement cover and share authentication. Medwell Asian J. Inf. Technol., 15: 2656-2662.

Liu, F. and C. Wu, 2011. Embedded extended visual cryptography schemes. IEEE Trans. Inform. Forensics Secur., 6: 307-322.

Mishra, S.K. and K. Biswaranjan, 2015. Extended visual cryptography for general access structures using random grids. Proceedings of the 2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Auguest 10-13, 2015, IEEE, Kochi, India, ISBN:978-1-4799-8790-0, pp: 1924-1929.

Noar, M. and A. Shamir, 1995. Visual Cryptography. In: Advance in Cryptography: Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques Perugia, De Santis, A. (Ed.). Springer, Netherlands, ISBN: 9783540601760, pp: 1-12.

Pahuja, S. and S.S. Kasana, 2017. Halftone visual cryptography for color images. Proceedings of the 2017 International Conference on Computer, Communications and Electronics (Comptelix), July 1-2,2017,IEEE,Jaipur,India,ISBN:978-1-5090-4709-3, pp: 281-285.

Quan, C., J. Jung, H. Lee, D. Kang and D. Won, 2018. Cryptanalysis of a chaotic Chebyshev polynomials based remote user authentication scheme. Proceedings of theInternational Conference on InformationNetworking (ICOIN), January 10-12, 2018, IEEE, Chiang Mai, Thailand, ISBN:978-1-5386-2291-9, pp: 438-441.

Wang, Z., G.R. Arce and G. Di Crescenzo, 2009. Halftone visual cryptography via. error diffusion. IEEE Trans. Inform. Forensics Secur., 4: 383-396.

Xiao, L., G. Xuan and Y. Wu, 2018. Research on an improved chaotic spread spectrum sequence. Proceedings of the IEEE 3rd International Conference on Cloud Computing and Big Data Analysis (ICCCBDA), April 20-22, 2018, IEEE, Chengdu, China, ISBN:978-1-5386-4302-0, pp: 420-423.

Zhou, Z., G.R. Arce and G. di Crescenzo, 2006. Halftone visual cryptography. IEEE. Trans. Image Process., 15: 2441-2453.