Halftone Visual Cryptography Scheme for Color Image using Dynamic Codebook and Chaotic Map

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

Abstract: Halftone visual cryptography is a method for encoding secret images into generated secure meaningful shares images. In this study, halftone visual cryptography scheme using dynamic codebook and chaotic maps technique is proposed for natural color images by using dynamic codebook technique the proposed method can be retrieved 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 Chebyshev 1D maps). This scheme gives 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, UIQI, SSIM and NCC metrics shown improvement in visual quality for shares images and ideal results for recovered color secret image.

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

INTRODUCTION

Information security plays 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 reveal 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 reason 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, College of Education, Mustansiriya 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 Chebyshev 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:**

**Input:**
- S/ color secret image
- C/ color cover image

**Output:**
- HSR, HSG, HSB/ halftone secret image
- HC/ halftone cover image

**Begin**
- Step 1: Apply error diffusion on S and C to generate HSR and HC
- Step 2: Split the HS image into three color bands HSR, HSG, HSB
- Step 3: 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 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.**

**Fig 1.** Burkes E-D coefficients matrix

**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**
- Step 1: Give for each pixel in HSR, (order, binary code (BIN))
- Step 2: BIN = 12 bits (the number 1’s bits must be equal number of 0’s bits)
- Step 3: Mask [4, 4] = BIN
- Mask [4, 4] = complement (BIN), the row indicated for flags
- Step 4: If Mask1 = 1 then place Mask2 to first location in HSR and place Mask2 to first location in HSB
- Step 5: Repeat 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 Chebyshev 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 homogencous 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:

8601
Fig. 2: Encoding step by using dynamic codebook: a) Input secret image; b) HSIR, HSG, HISB (histogram halftone secret image for RGB color bands), respectively and c) Dynamic codebook mechanism

\[ X_n(n+1) = \mu X_n(1 - X_n) \]  

(1)

where, \( X \sim [0, 1], \mu \) represent bifurcation parameters, if we change the value of \( \mu \) the logistic map behavior is changes drastically. The logistic maps became in chaotic stats when \( 3.5695 < \mu < 4 \) sequence of the logistic function has the features of simple shapes and sensitivity to initial conditions (Xiao et al., 2018).

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

Definition 1: The Chebyshev polynomial in degree \( n \) is determined as:

\[ T_n(x) = \cos(n \arccos(x)) \]

where, \( n \) is integer number, \( x \sim [-1, 1] \).

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

\[ T_n(x) = T_n(T_{n-1}(x)) = T_n(T_{n-2}(x)) \]

Definition 3: The Chebyshev polynomial in \( n \) degree, present:

\[ x, T(x) \]

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
   m/number of rows in periods table which equal 32
   x0, y0/initial value for logistic and Chebyshev function
   xBlock1 and 2/Boolean array

Output: set of random location xkey

Begin: Step1: Create Epron
   Step 2:
   Step 2-1: for i = 0 to xwidth
            Logistic value = r * (x0 + (1-x0))
            swap(x0, Logistic value)
            loc = 0
            for n = 0 to m
            if (Logistic value > = index[n] & Logistic value < index[n+1])
               loc = n
               end for
            end for
   Step 2-2: while (true) {
            Chebyshev value = cos(k * (cos(x) x0))
            swap(x0, Chebyshev value)
            xBlock2 = xBlock2 xBlock1(2+D2B(2+(CHEBYSHEV value, FixedBlock)
            if (xBlock1.Length > 32) then end loop)/
   while
   Step 2-3: Determine two equal parts in Epron each part represent 32 locations and assigned the pointer i for part i and pointer j for part j
   for i = 0 to Epron size/2
   if (xkey = Epron[i]) then swap
   (Epron[i], Epron[j])
   /'
   end for
   Step 2-4: if(k * (xwidth), xwidth) != 1)
   {
   xkey = Epron[32] 
   if (xkey == -1) Then find nearest value to Epron[loc] != -1 and assigned to xkey and replaced value of this location in Epron by -1 Else Epron [loc] = -1
   End if
   Else xkey = Epron [loc]
   k = k+1
   Epron[loc] = -1
   /'
   End if
   /'
   Step 3: Repeated step 2 until get all location that need to embedded all secret pixels
   End algorithm

8602
Figure 3 shown, the result of algorithm 5 which is represent random location by using logistic and Chebyshev 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, HIC/Halftone Cover image
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 Chebyshev chaotic system when value of Fixedblock = 4. Figure 8 shown, the generated random location by using Logistic and Chebyshev chaotic system when value of Fixedblock = 8. Figure 9 shown, the generated random location by using logistic and Chebyshev chaotic system when value of Fixedblock = 10.

---

**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:

1. Determined first q− cell in Share 1 and Extract value of (z)/− is variable dedicated to q− cell.

Step 1: z = 0

Step 2: For m = 1–4

   x = 1, y = j

   If MC[x, y] = 1 Then z = q[m, n], q−[m, n] = q[m, n], q−[4, 1] = q−[4, 2]

   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] = q[m, n]

   End if

Step 3: Repeated step 1 to 2 to embedded all Mask cells MC[x, y] into all halftone cell (q−[m, n]) in HSI to generate random share

End algorithm

---

**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 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):

$$MSE = \frac{1}{M \cdot N} \sum_{i=1}^{M} \sum_{j=1}^{N} [(I(i,j) - k(i,j))^2]$$
Figure 10: Generate meaningful share images: a) Cover images before embedded the SIP and b) Cover images after embedded the SIP.

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

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

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:

$$UQI = \frac{4\sigma_x\sigma_y}{\sigma_x^2 + \sigma_y^2} \frac{X^2 + Y^2}{2}$$

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

Figure 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):

$$SSIM = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{\mu_x^2 + \mu_y^2 + C_1(\sigma_x^2 + \sigma_y^2 + C_2)}$$

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):

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

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
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 Chebyshev 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 Brucker 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 SIF 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


