Visual Cryptography Vs Bit Level Secret Sharing For Image Encryption

Musaab R. Abdulrazzaq*

Received on:7/7/2009
Accepted on:3/12/2009

Abstract

Secret sharing is a scheme used to distribute secret among a group of users. Rather than making duplicated copies of secrets among users, the secret is divided into a number of pieces, called shares. The secret can be revealed if a certain number of user shares are combined. The method proposed here (i)utilizes bit-level decomposition and stacking operations to both encrypt and decrypt B-bit image, (ii) preserves all the features of traditional (k, n) sharing schemes, (iii) allows for perfect reconstruction of the input B-bit image, (iv) encrypts binary, gray-scale and color images, and (v) can be effectively implemented either in software or hardware.

Keywords: cryptography; Secret sharing; shares; Image encryption; Bit-level.

مقارنة بين التشفير المرئي والتشفير على مستوى البتات لخوارزميات مشاركة الاسرار لتشفير الصور

الخلاصه

تقترح خوارزميات مشاركة الاسرار الى تجزئة السر الى عدة اجزاء (shares) وتوزيعها الى مجموعة من المستخدمين بدلا من توزيع نفس النسخة، يمكن استعادة السر عند توفر جميع الاجزاء او عدد محدد منها. في هذا البحث تم اقتراح خوارزمية جديدة تنفذ على مستوى البتات (التجزئة والتجميع) تحتوي على جميع خصائص خوارزميات مشاركة الاسرار (k, n) وتمتاز بانها سهلة التنفيذ ومناسبة لجميع انواع الصور (الثنائية والرمادية والملونة) ويمكن تنفيذها بواسطة البرامجيات او المكونات المادية.

1-Introduction

Secret sharing is one type of key establishment protocols. The Trusted Authority (TA) divides the secret into pieces and distributes the pieces to different users. These pieces are called shares. Shares contain partial information about the secret. However, shares are constructed in such a way that although the secret can be reconstructed by combining a number of shares, simply examining individual user's share will not reveal the secret information at all [1]. Secret sharing-based image encryption technology can be utilized to secure data transmission in multimedia networks and mobile public networks which are used for exchange of private images such as scanned (e.g. financial) documents and digital personal photographs. The secret sharing scheme proposed here offers a new approach to secret sharing encryption which differs

* College of Sciences, University of Al Mustansiriya /Baghdad

https://doi.org/10.30684/etj.28.7.6
2412-0758/University of Technology-Iraq, Baghdad, Iraq

significantly from traditional image sharing schemes in visual cryptography. Unlike past image sharing schemes, the proposed {k, n} technique operates directly on the bit level of the digital input image. If the input image with the B-bit code word representation of the samples is decomposed into B bit-levels (planes), each one can be viewed as a binary image. By stacking individually encrypted bit planes, the scheme produces the B-bit shares useful for secure distribution over the untrusted public networks.The decryption function recoversthe original B-bit image content unchanged and without the need for expensive postprocessing operations. The decrypted output is readily available in digital form, and there is no requirement for external hardware (overhead projector) or manual intervention needed. This feature in conjunction with the overall simplicity of the approach make the proposed input-agnostic solution attractive for real time. [2]

2- Background on visual cryptography

Visual cryptography was originally proposed for the problem of secret sharing. Secret sharing is one of the early problems to be considered in cryptography. In a (k, n)-threshold problem, a secret is divided into n pieces. With any k of the n pieces, the secret can be perfectly reconstructed, while even complete knowledge of k-1 pieces reveals absolutely no information about the secret. Visual cryptography illustrated a new paradigm to solve the (k,n) problem. It was originally proposed by Naor and Shamir [3]. The original scheme generates n images (known as shares) based on the secret message (the original image) which can be printed on n transparencies. The original message can then be recovered if any k or more than k of the transparencies are stacked together, but no information about the original image can be gained if fewer than threshold number of k transparencies are stacked. Visual cryptography is a unique technique in the sense that the encrypted messages can be decrypted directly by the human.[3,4]

To encrypt a $(k1 \times k2)$ binary image using visual cryptography, each binary pixel $r(i,j)$ (i.e. $r(i,j)=1$ for white and $r(i,j)= 0$ for black) is handled separately via an encryption function $FEnc(\cdot)$ to produce a $(m1\times m2)$ block of black and white pixels in each of the n shares. Thus, a $(k1\times k2)$ input binary image is encrypted into (n) binary shares S1, S2, . . , Sn each one with resolution of $(m1k1\times m2k2)$ pixels. Since the arrangement of the pixels varies from block to block, it is impossible to recover the useful information without accessing a predefined number of shares.[4,5]

Let $FEnc(\cdot)$ be the encryption function which maps a reference binary pixel $r(i,j)$ located at position (i,j) in the original image into $(m1\times m2)$ sized blocks in the various shares. Assuming for simplicity a basic (2, 2) scheme with (2×2) blocks, the encryption process is given by:

For each pixel $r(i,j)$ in the binary image

$F_{Enc}(r(i,j))$

{if $r(i,j) = 1$ (white) then

Select random block from C (Fig. 1) and insert the block at locations:

Share1 $[(2i-1,2j-1), (2i-1,2j), (2i,2j-1), (2i,2j)]$

Share2 $[(2i-1,2j-1), (2i-1,2j), (2i,2j-1), (2i,2j)]$

Else {b(i,j) = 0}
Select random block from C and
insert the block at locations:
Share1 [(2i−1,2j−1), (2i−1,2j), (2i,2j −1), (2i,2j)]
insert the complement of C at locations:
Share2 [(2i−1,2j−1), (2i−1,2j), (2i,2j −1), (2i,2j)] }

as shown in Fig. (1)

The size of the basis matrices depends on the expansion factor m1m2 and the number of participants, which is given by n. Since m1m2 represents the factor by which each share is larger than the original image, it is desirable to make m1m2 as small as possible [6,7].

For a (2, 2) scheme considered here, each pixel in Share1 is equivalent to each pixel in Share2 if r(i, j) = 1, and each pixel in Share1 should complement each pixel in Share2 if r(i,j)=0.

The decryption function FDec (Share1(u,v), Share2(u,v)) is defined as follows:

```
for i = 1 to k1      { k1 = u/2 }
for j = 1 to k2      {k2 = v/2 }
if  Share1(2i-1, 2j-1) = Share2(2i-1, 2j-1) then
        b(i, j) =1
    else
        b(i, j) =0
next j:  next i
```

Where (u) is the height of share1 & share2 (2*k1) and (v) is the width of share1 & share2 (2*k2) and b is the decrypted image as shown in figure (1).

3- Bit level based secret sharing (Coding algorithm)

The coding algorithm of our proposed system:

Step1: Read a digital image (k1 x k2) with B-bit/pixel. (in this paper B=8)

Step2: Decompose the input image to eight binary images, ranging from (0) for the least significant bit (LSB) to (7) for the most significant bit (MSB) (b0 … b7) as shown in figure (2). [8]

Step3: implement the following procedure:

```
for plane = 0 to 7
for  i = 1  to  height of image
for  j = 1  to  width of image
 if  b(i, j, plane) = 0  (black) then
  select random block from C and
  insert the block at locations:
      S1[(2i−1,2j−1,plane),
         (2i−1,2j, plane),
         (2i,2j−1, plane),
         (2i,2j, plane)]
    insert complement of the block
    at location:
      S2 [(2i−1,2j−1,plane),
         (2i−1,2j, plane),
         (2i,2j−1, plane),
         (2i,2j, plane)]
   else   { white }
     select random block from C
    and insert the block at locations:
      S1 [(2i−1,2j−1,plane),
         (2i−1,2j, plane),
         (2i,2j−1, plane),
         (2i,2j, plane)]
      S2 [(2i−1,2j−1,plane),
         (2i−1,2j, plane),
         (2i,2j−1, plane),
         (2i,2j, plane)]
  next j : next i :  next plane
```

Step4: compose S1(u, v, 0-7) and S2 (u, v, 0-7) using equation 4 & 5:

$$Share1(u,v)= S1(u,v,7)*2^7+ S1(u,v,6)*2^6 + \cdots + S1(u,v,0)*2^0 \quad \ldots(4)$$

$$Share2(u,v)= S2(u,v,7)*2^7 + S2(u,v,6)*2^6 + \cdots + S2(u,v,0)*2^0 \quad \ldots(5)$$

Where u = 2*image height & v= 2 * image width As shown in figure (3)

Decoding algorithm:
To faithfully decrypt the original B-bit image from its shares, the decryption function must satisfy the perfect reconstruction property meaning that the output should be identical to the original input. This can be obtained only if the encryption and decryption operations are reciprocal.
Step1: Decompose each input share1 and share2 to eight binary images (2k1 x 2k2), ranging from (0) for the least significant bit (LSB) to (7) for the most significant bit (MSB).
Step2: implement the following procedure:

```
for plane = 0 to 7
for  i  = 1  to  k1
for  j  = 1  to  k2
   if Share1(2i-1,2j-1,plane)=
      Share2(2i-1, 2j-1, plane)    then
         b(i, j, plane) =1
   else
         b(i, j, plane) =0
 next j : next i:  next plane
```

Step3: the eight binary images b (k1 x k2) are constituted by bit-level stacking using (equation 4) to obtain the original image.

4- Visual cryptography vs bit level secret sharing

Visual cryptography of the binary image indicates that: (i) the decrypted image is darker, and (ii) the input image is of quarter size compared to the decrypted output.
Visual cryptography (iii) cannot provide perfect reconstruction, either in terms of pixel intensity or spatial resolution, and (iv) is not appropriate for real-time applications as shown in fig(5). Thus, an alternative solution is needed [9,10].

The method proposed here (i) utilizes bit-level decomposition and stacking operations to both encrypt and decrypt B-bit image, (ii) preserves all the features of traditional {k, n} sharing schemes, (iii) allows for perfect reconstruction of the input B-bit image, (iv) encrypts binary, gray-scale and color images, and (v) can be effectively implemented either in software or hardware as shown in fig. (6,7) .

5- Implementation

We use MATLAB language to implement visual cryptography and B-bit-level algorithm, the following figures (5,6,7) offers a visual comparison between two methods.

6. Conclusions

A B-bit secret sharing framework that affords perfect reconstruction of the encrypted image input was introduced. The method proposed here (i) utilizes bit-level decomposition and stacking operations to both encrypt and decrypt B-bit image, (ii) preserves all the features of traditional {k, n} sharing schemes, (iii) allows for perfect reconstruction of the input B-bit image, (iv) encrypts binary, gray-scale and color images, and (v) can be effectively implemented either in software or hardware.

7. visual cryptography researches

There has been a steadily growing interest in visual cryptography. Despite its appearance of being a simple technique, visual cryptography is a secure and effective cryptographic scheme. Since the origin of this new paradigm, various extensions to the basic scheme have been developed to improve the contrast and the areas of application have also been greatly expanded.

In [1'], the construction of (n,n)-VCS was extended for (k,n)-VCS. In 1996, the same authors introduced the idea of cover based semi-group to further improve the contrast [2']. Ateniese et al. [3'] provided the first construction of (2, n)-VCS having the best possible contrast for any n<=2. Blundo et al. [4'] provided a contrast optimal (3,n)-VCS and gave a proof on the upper bound on the contrast of any (3,n)-VCS. [1'] first considered the problem of concealing the existence of the secret image. [5'] provided a general solution for that problem.

The random nature of secret shares makes shares unsuitable for transmission over an open channel. [5'] used a modified scheme to embed some meaningful images into the shares. [6'] used different moiré patterns to visualize the secret instead of different gray levels.

As far as extending to color images goes, [7'] provided a primitive scheme for images of 24 colors. Hou [8'] then proposed a novel approach to share color images based on halftoning. Other interesting topics include visual authentication [9'] and watermarking based on visual cryptography [10']. Recently, there has been an attempt to build a physical visual cryptographic system based on optical interferometry [11']. However, all of these works result in a decrypted image of reduced quality.

Visual cryptography researches:

[1'] M. Naor and A. Shamir, "Visual cryptography," in Advances in Cryptology EUROCRYPT'94, A. D. Santis., Ed., vol. 950. Springer-Verlag, 1995, pp. 1–12.

[2'] M. Naor and A. Shamir, "Visual cryptography 2: Improving the contrast via the cover base," 1996, a preliminary version appears in "Security Protocols", M. Lomas ed. Vol. 1189 of Lecture Notes in Compute Science, Springer-Verlag, Berlin, pp.197-202, 1997.

[3'] A. D. S. G. Ateniese, C. Blundo and D. R. Stinson, "Constructions and bounds for visual cryptography," in 23rd International Colloquium on Automata, Languages and Programming, ser. Lecture Notes in Computer Science, F. M. auf der Heide and B. Monien, Eds., vol. 1099. Berlin: Springer-Verlag, 1996, pp. 416–428.

[4'] C. Blundo, P. D'Arco, A. D. Snatis, and D. R. Stinson, "Contrast optimal threshold visual cryptography schemes," SIAM Journal on Discrete Mathematics, available at: http://citeseer.nj.nec.com/blundo98contrast.html, vol. 16, no. 2, pp. 224–261, April 1998.

[5'] G. Ateniese, C. Blundo, A. D. Santis, and D. Stinson, "Extended schemes for visual cryptography," Theoretical Computer Science, vol. 250, pp. 143–161, 2001.

[6'] Y. Desmedt and T. V. Le, "Moire cryptography," in the 7th ACM Conference on Computer and Communications Security'00, Athens, Greece, 2008.

[7'] V. Rijmen and B. Preneel, "Efficient color visual encryption for shared colors of benetton," 1996, EUCRYPTO'96 Rump Session. Availabe at http://www.iacr/org/conferences/ec96/rump/preneel.ps.

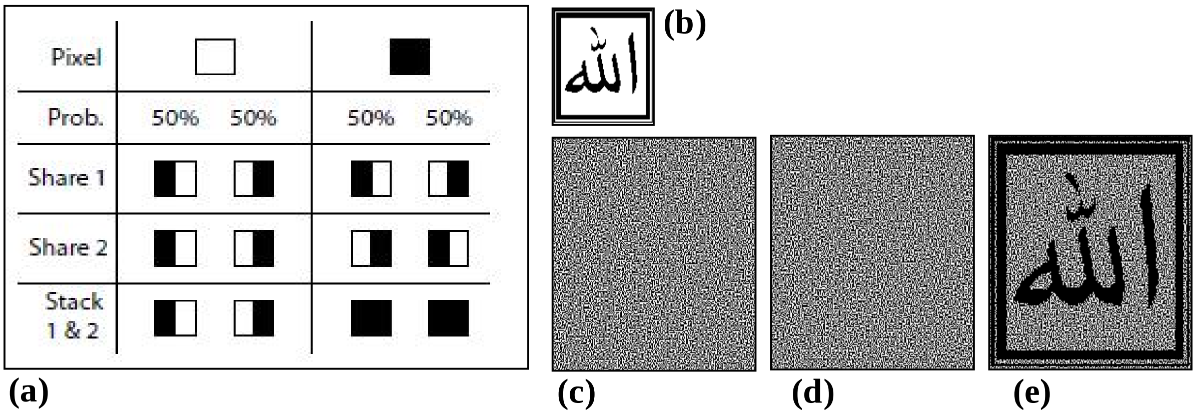
[8'] Y. C. Hou, C. Y. Chang, and S. F. Tu, "Visual cryptography for color images based on halftone technology," in International Conference on Information Systems, Analysis and Synthesis. World Multiconference on Systemics,

Cybernetics and Informatics. Image, Acoustic, Speech And Signal Processing: Part II, 2007.
[9'] M. Naor and B. Pinkas, “Visual authentication and identification,” Lecture Notes in Computer Science, vol. 1294, pp.322–336, 1997. [Online]. Available: citeseer.nj.nec.com/67294.html
[10'] Q. B. Sun, P. R. Feng, and R. Deng, in International Conference on Information Technology: Coding and Computing (ITCC ’01), available at: http://dlib.computer.org/conferen/itcc/1062/pdf/10620065.pdf, Las Vegas, April 2001.
[11'] S.-S. Lee, J.-C. Na, S.-W. Sohn, C. Park, D.-H. Seo, and S.-J. Kim, “Visual cryptography based on an interferometric encryption technique,” ETRI Journal, vol. 24, pp. 373–380, 2007, available at http://etrij.etri.re.kr/etrij/pdfdata/24-05-05.pdf. January 6.

References

[1] ZhenMing Jiang, Chao Li, XiaoTing Sun Visual Cryptography December 17, 2005
[2] R. Lukac, K.N. Plataniotis, Colour image secret sharing, IEE Electron. Lett. 40 (9) (2004) 529–530.
[3] Moni Naor and Adi Shamir. Visual Cryptography. Eurocrypt 94, 1994.
[4] Jim Cai, A Short Survey On Visual Cryptography Schemes, 2008.
[5] K.Y. Chen, W.P. Wu, and C.S. Laih. On the (2,2) visual multi-secret sharing schemes, 2008.
[6] M. Nakajima and Y. Yamaguchi, “Extended Visual Cryptography for Natural Images,” Journal of WSCG, vol. 10, no. 2, 2007.
[7] D. Jin, “Progressive color visual cryptography,” Masters degree thesis, School of Computing, National University of Singapore, Singapore, July 2009.
[8] Gonzalez C. Wintz P. 1987 “Digital image processing, 2nd edition Addison-Wesley, MA.
[9] Carlo Blundo and Alfredo De Santis and Douglas R. Stinson. On the Constrast in Visual Cryptography Schemes. Journal of Cryptology 12, pages 261–289, 1999.
[10] J.C. Hou, Visual cryptography for color images, Pattern Recognition 36 (7) (2003) 1619–1629.

$$C = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \quad \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$$



Figure(1) a. Visual Cryptography strategy. b. input binary image (k1 x k2). c. Share1(u, v). d. Share2 (u, v). e. Decrypted image.

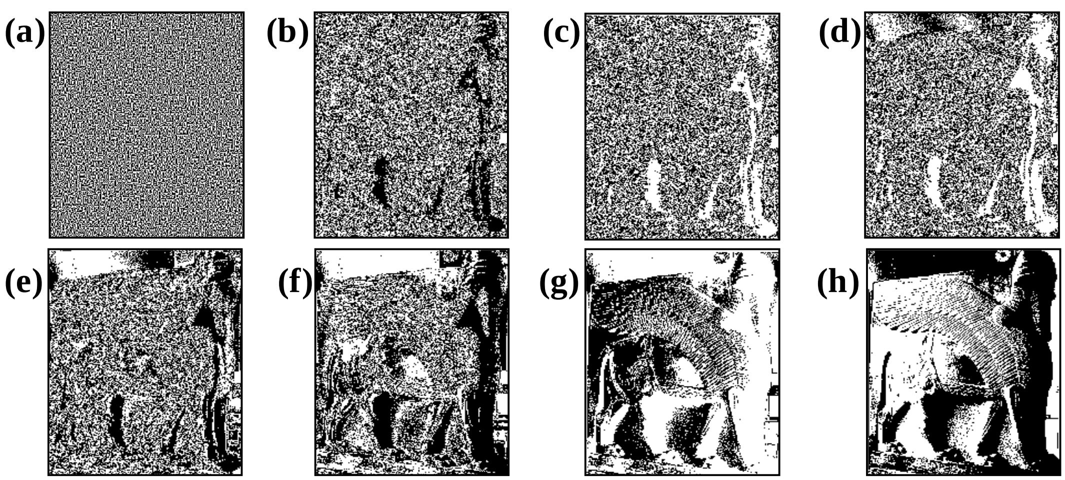
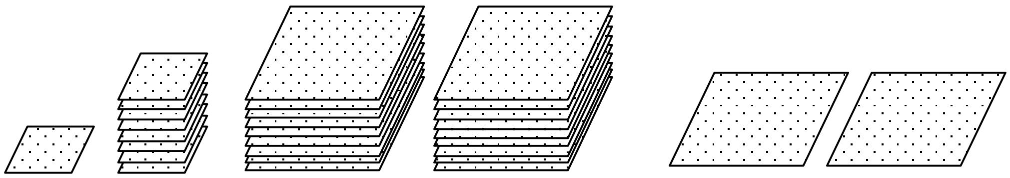


Figure (2) Binary images corresponding to the bit-levels of the gray-scale (B =8) image: (a) b =8, (b) b =7, (c) b =6, (d) b = 5, (e) b = 4, (f) b = 3, (g) b = 2, (h) b = 1.



(a) (b) b(0- (c) S1 (u, v, 0-7) (d) S2 (u, (e) Share1(u,v)..

Figure (3) coding algorithm

a. 8-bit gray scale image (k1xk2) b. step2 decompose the image to 8 binary image (k1xk2)

c. step 3 generate S1 (u,v,0)… S1(u,v,7)

d. generate S2 (u,v,0) … S2(u,v,7)

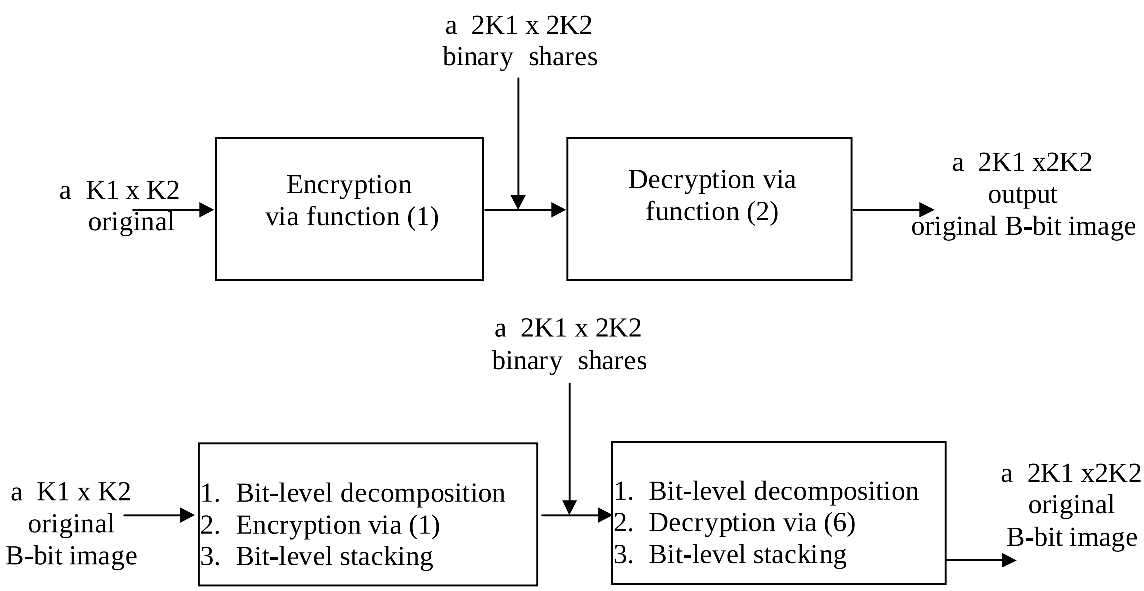
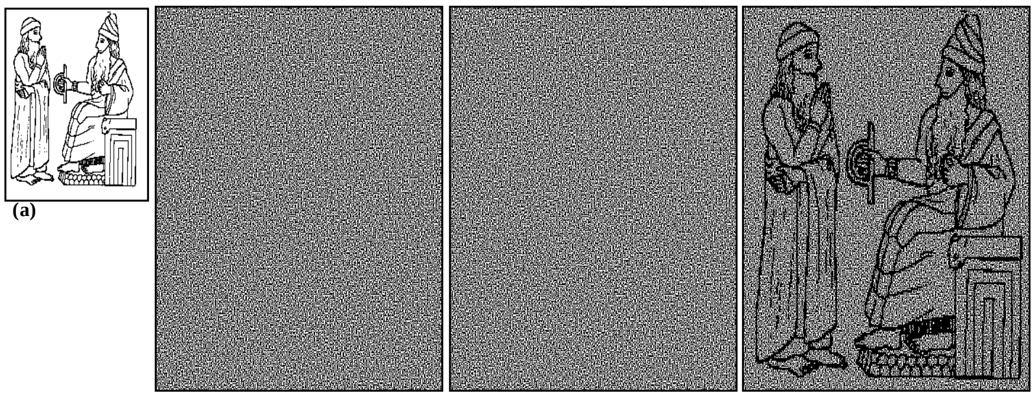


Figure (4) Visual cryptography algorithm VS bit-level algorithm

(b) (c) (d)



(a)

Figure (5) {2, 2} visual cryptography applied to King Hamorabi binary input image:
(a) a K1 × K2 original binary image, (b) a 2K1 × 2K2 share S1, (c) a 2K1 × 2K2 share S2, (d) a 2K1 × 2K2 decrypted binary (output) image.

(b) (c)

(a) (d)

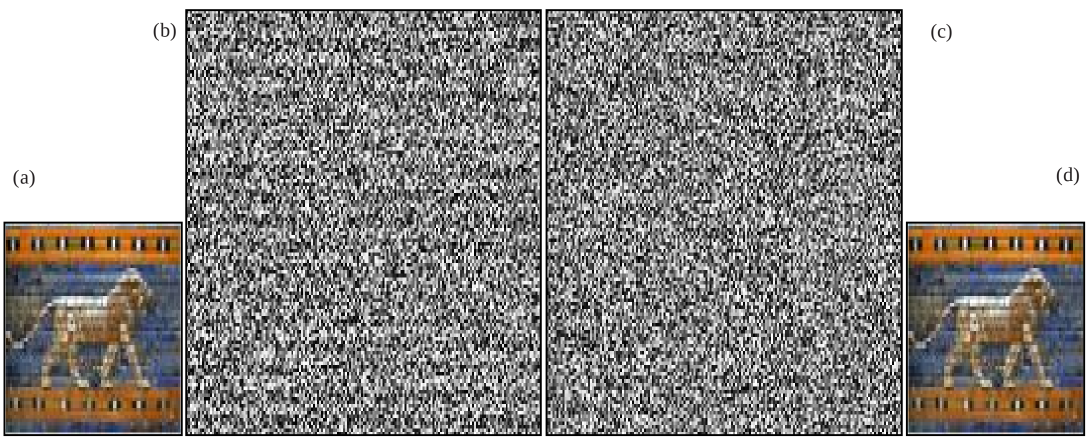


Figure (6) The proposed B-bit {2, 2}-secret sharing framework applied to the gray-scale input:
(a) a K1 × K2 original gray-scale image, (b) a 2K1 ×2K2 gray-scale share S1, (c) a 2K1 ×2K2 gray-scale share S2, (d) restored output.

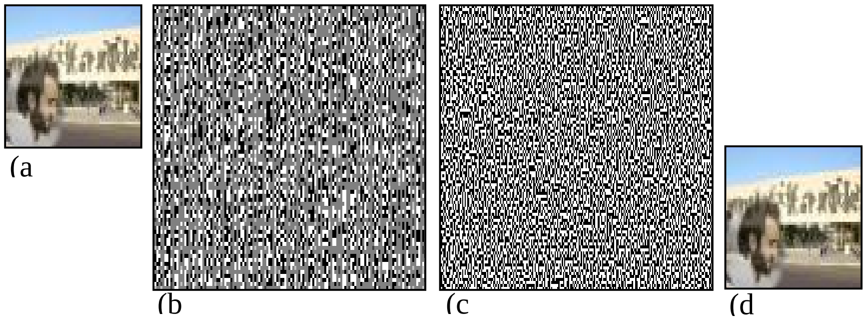


Figure (7) The proposed *B*-bit {2, 2}-secret sharing framework applied to color input image :

(a) a $K1 \times K2$ original color image. (b&c) $2K1 \times 2K2$ gray-scale shares $S1$, $S2$.
(d) restored output using shares $S1$ & $S2$.