Performance Evaluation Of Extended Visual Cryptography Schemes With Embedded Extended Visual Cryptographic Scheme.

Miss. Asha S.N. [1], Dr.Shreedhara .K.S.M.Tech., Ph.D [2], Smt. Anitha G. BE, ME[3],

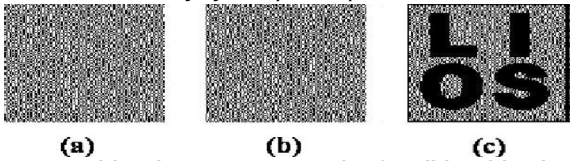
Abstract: Visual cryptography scheme (VCS) is a kind of secret sharing scheme which allows the encoding of a secret image into n shares that distributed to n participants. The beauty of such scheme is that a set of qualified participants is able to recover the secret image without any cryptographic knowledge and computation devices. Extended visual cryptography scheme (EVCS) is a kind of VCS which consists of meaningful shares (compared to the random shares of traditional VCS). Intent of this paper is the study and construction of EVCS which is realized by embedding random shares into meaningful covering shares, and we call it the embedded extended visual cryptography scheme (embedded EVCS). Experimental results compare some of the well-known EVCS's proposed in recent years systematically, and show that the proposed embedded EVCS has competitive visual quality compared with many of the well-known EVCS's in the literature. Besides, it has many specific advantages against these well-known EVCS's respectively.

Keywords: Secret sharing, cryptography, encoding, Embedded, Extended visual cryptography scheme.

I. Introduction

The basic principle of visual cryptography scheme (VCS) was first introduced by Naor andShamir. VCS is a kind of secret sharing scheme [1, 2] that focuses on sharing secret images. Theidea of the visual cryptography model proposed in [3] is to split a secret image into two random shares (printed on transparencies) which separately reveals no information about the secret imageother than the size of the secret image. The secret image can be reconstructed by stacking the twoshares. The underlying operation of this scheme is logical operation *OR*. In general, a traditional VCStakes a secret image as input, and outputs $n$shares that satisfy two conditions: (1) any of shares can recover the secret image;(2) Any forbidden subset of shares cannot obtain anyinformation of the secret image other than the size of the secret image. An example of traditional(2, 2)-VCS can be found in the following Figure 1, where, generally speaking, a (k, n)-VCS meansany $k$out of $n$shares could recover the secret image. In the scheme of Figure 1, shares (a) and (b) are distributed to two participants secretly, and each participant cannot get any information aboutthe secret image, but

after stacking shares (a) and (b), the secret image can be observed visuallyby the participants.



(a) (b) (c)

(a) Figure 1: An example of traditional (2, 2)-VCS with image size 128×128.

Many other applications of VCS, other than its original objective (i.e. sharing secret image), havebeen found, for example, authentication and identification [4], watermarking [5] and transmittingpasswords [6] etc.

The term of extended visual cryptography scheme (EVCS) was first introduced by Naor et al.in [3], where a simple example of (2, 2)-EVCS was presented. Generally, an EVCS takes a secret image and $n$original share images as inputs, and outputs $n$shares that satisfy the following three conditions:

(1) Any qualified subset of sharescan recover the secret image; (2) Any forbidden subset of shares cannot obtain any information ofthe secret image other than the size of the secret image; (3) All the shares are meaningful images.Examples of EVCS can be found in the experimental results of this paper, such as Figures2-9.

There have been many EVCS's proposed in the literature. Droste [7], Ateniese et al. [8] and Wang et al. [9] proposed three EVCS's, respectively, by manipulating the share matrices.Nakajima et al. [10] proposed a (2, 2)-EVCS for natural images. Tsai et al. [11] proposed a simpleEVCS, where its shares were simply generated by replacing the white and black sub-pixelsin a traditional VCS share with transparent pixels and pixels from the cover images respectively.Furthermore, Zhou et al. and Wang et al. [12–14] presented an EVCS by using halftoning techniques.Their methods made use of the complementary images to cover the visual information ofthe share images. Recently, Wang et al. proposed three EVCS's by using error diffusion halftoningtechnique [15] to obtain nice looking shares. Their first EVCS also made use of complementaryshares to cover the visual information of the shares as the way proposed in [12]. Their secondEVCS

imported auxiliary black pixels to cover the visual information of the shares. In such away, each qualified participants did not necessarily require a pair of complementary share images.Their third EVCS modified the halftoned share images and imported extra black pixels to coverthe visual information of the shares.

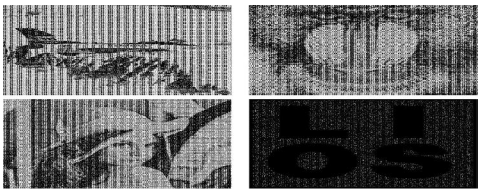


Fig. 2. Shares and the recovered secret image of an embedded (3, 3)-EVCS after reducing the black ratios, the image size is 1024 x 1024**.**

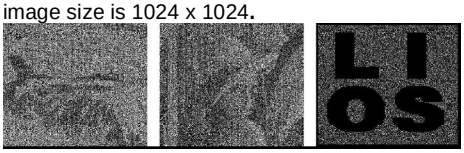


Fig. 3. Experimental results of (2, 2)-EVCS proposed in [7]–[9]. The size of all the images is 768 x 768.

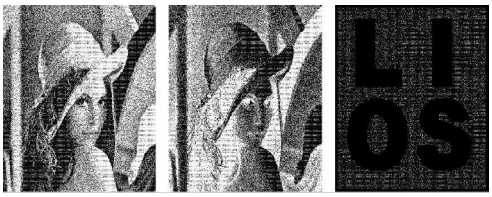


Fig. 4. Experimental results of (2, 2)-EVCS proposed in [15], [12]. The size of all the images is 768 x 768.

Fig. 5. Experimental results of Method 2 for (2, 2)-EVCS proposed in [13]. The size of all the images is 768 x 768.

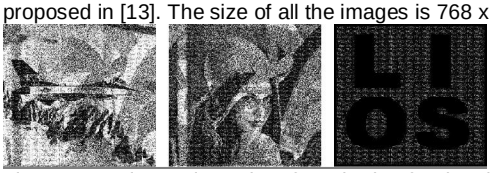


Fig. 6. Experimental results of Method 3 for (2, 2) - EVCS proposed in [13]. The size of all the images is 768 x 768.

However, the limitations of these EVCS's mentioned above are obvious. The first limitation isthat the pixel expansion is large. Thesecond limitation is the bad visual quality of both the shares and the recovered secret images.

Fig. 7. Proposed (2, 2)-EVCS. The size of all the images is 768 x 768.

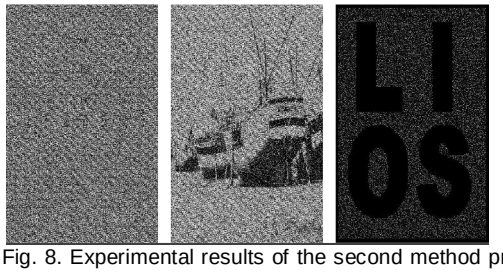


Fig. 8. Experimental results of the second method proposed in [13] for fine share images. The size of all the images is 768 x 768.

Fig. 9. Proposed (2, 2)-EVCS for fine share images. The size of all the images is 768 x 768.

This paper proposes an embedded EVCS scheme with overall good properties. Comparisons of properties of our proposed scheme with some well-known EVCSs can be found in Section IV, where we will show that our scheme has competitive visual quality compared with many of the well-known EVCSs. Besides, our EVCS has many specific advantages against these well-known EVCSs, respectively. The rest of this paper is organized as follows: In Section II, we introduce the formal definition of embedded EVCS, and give the main idea about our construction. In Section III, we embed the traditional VCS into the covering shares and discuss the bounds of our scheme. Lastly, in Section V, we conclude the paper.

II. A sketch and the main idea of the proposed embedded EVCS

In this section, we will give an overview of our construction. First we introduce the formal definition of embedded EVCS.

Definition1 (embedded EVCS)Denote $_0$*and* $_1$*as the basis matrices of a traditional VCS with access structure* (Γ , Γ) *and pixel expansion . In order to encode a secret image , the dealer takes grey-scale original share images as inputs, and converts them into covering shares which are divided into blocks of sub-pixels (≥). By embedding the rows of* $_0$*and* $_1$ *(after randomly permuting their columns) into the blocks, the embedded EVCS outputs shares* $_0$, ⋯,$_{n-1}$, *and there exist values* {$\hbar$: $\in\Gamma$ }, *and satisfying:*

1. The stacking result of each block of a qualified subset of shares can recover asecret pixel. More precisely, if = { $_1$, ⋯, } ∈ Γ , *denote* $_1$,⋯, *as the blocks at the same position of the shares* $_1$, ⋯, , *then for a white secret pixel, the* OR *of* $_1$, ⋯, *is a vector that satisfies* ( ) ≤ $\hbar$ − , *and that for a black secret pixel, it satisfies* ( ) ≥ $\hbar$.

2. Part of the information of the original share images is preserved in the shares. Define = (−)/ be the ratio of the information of the original share images that preserved in the shares, and it satisfies >0.

In Definition 1, the first condition ensures that the secret image can be visually observed by stacking a qualified subset of shares. The second condition ensures that the shares are allmeaningful in the sense that parts of the information of the original share images are preserved. The idea of our embedded EVCS contains two main steps:

(1) Generate covering shares, denoted as $_0, _1, \cdots, _{-1}$;

(2) Generate the embedded shares by embedding the corresponding VCS into the covering shares, denoted as $_0, _1, \cdots, _{-1}$.

III. Embedding the corresponding VCS into the covering shares

Algorithm 1 *The embedding process:*

Input: *The covering shares constructed, the corresponding VCS ($_0, _1$) with pixel expansion and the secret image .*

Output: *The embedded shares $_0, _1, \cdots, _{-1}$.*

Step 1: *Dividing the covering shares into blocks that contain (≥) sub-pixels each.*

Step 2: *Choose embedding positions in each block in the covering shares.*

Step 3: *For each black (resp. white) pixel in , randomly choose a share matrix ∈ $_1$ (resp. ∈ $_0$).*

Step 4: *Embed the sub-pixels of each row of the share matrix into the embedding positions chosen in Step 2.*

The diagram of Algorithm 1 can be found in Fig. 11.

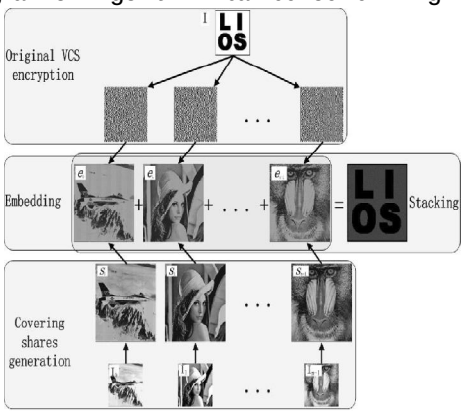


Fig. 11. Diagram of Algorithm 1.

III. Experimental results and comparisons.

In this section, we compare the embedded EVCS with many of the well-known EVCS's inthe literature.

Fig. 10. Original share images (airplane, baboon, Lena, ruler, and boat) and the secret image.

First, we give the original images that will be used in the paper (Fig. 10): Lena, airplane, baboon, ruler, boat, and the secret image. The sizes of these images are 256 x 256; they willbe scaled to their proper size when necessary.

We provide two well-known objective numerical measurementsfor the visual quality, the peak signal-to-noise ratio (PSNR) and the universal quality index (UQI) [16]. In thispaper, the PSNR is adopted to assess the distortion of each shareimage with its original halftoned share image (i.e., withoutthe darkening process). In such a way, the PSNR values inTables IX and X can reflect the effects of a combination of thefollowing possible processes in EVCSs: darkening, embedding,and modification. The PSNR is defined as follows:

$$= 10 \log \frac{255^2}{\text{MSE}} \quad (1)$$

Where MSE is the mean squared error. The UQI is adoptedto assess the distortion of each share image with its original ray-scale share image (after being scaled to the size of shares).Hence, the UQI value can reflect the effect of the halftoningprocess besides that of the darkening, embedding and modification processes in EVCSs. The formal definition of UQI can befound in [16]. In this paper, the block size of UQI is set to be 8for all the experiments.

The original halftoned share images ofZhou *et al.* and Wang *et al.*'s schemes in Figs. 4, 5, 6, and 8are generated by the blue noise halftoning technique and errordiffusion halftoning technique on the original share images inFig. 10 directly.

TABLE IX
OBJECTIVE NUMERICAL MEASUREMENTS OF FIG. 2

	Content interaction	PSNR share 1	PSNR share 2	PSNR share 3	UQI share 1	UQI share 2	UQI share 3	Contrast	PE'	PE''
Fig. 5	No	8.69db	8.62db	8.93db	0.0311	0.0699	0.0215	1/16	16	16

TABLE X

OBJECTIVE NUMERICAL MEASUREMENTS OF FIGS. 3, 4, 5, 6, 7, 8, AND 9

	Content interaction	PSNR share 1	PSNR share 2	UQI share 1	UQI share 2	Contrast	PE'	PE"
Fig. 6	No	3.19db	3.77db	0.0008	0.0032	2/9	9	9
Fig. 7	Yes	9.54db	0.51db	0.0445	-0.0315	1/9*	9	9
Fig. 8	No	3.16db	4.08db	0.0254	0.0304	1/9	9	9
Fig. 9	Yes	4.62db	4.11db	0.0578	0.0332	1/9	9	9
Fig. 10	No	5.67db	6.01db	0.0293	0.0281	1/9	9	9
Fig. 11	No	2.72db	3.61db	0.0438	0.0270	1/9	9	9
Fig. 12	No	3.36db	7.15db	0.0630	0.0289	1/9	9	9

IV. Conclusion

The shares of the proposed scheme are meaningfulimages, and the stacking of a qualified subset of shares will recover the secret image visually. According to the comparisons with many of the well-known EVCS in theliterature [7, 8, 10, 12, 13, 15], the proposed embedded EVCS has many specific advantagesagainst different well-known schemes, such as can deal with grey-scale input images, has smallerpixel expansion, always unconditionally secure, does not require complementary share images,one participant only needs to carry one share and can be applied for general access structure.Furthermore, our construction is flexible in the sense that there exist two trade-offs between theshare pixel expansion and the visual quality of the shares and between the secret image pixelexpansion and the visual quality of the shares.

Comparisons on the experimental results show that, the visual quality of the share of theproposed embedded EVCS is competitive with that of many of the well-known EVCS's in theliterature.

References

[1] A. Shamir. How to share a secret.In *Communications of the ACM*, volume 22 (11), page612C613, 1979.

[2] G. R. Blakley. Safeguarding cryptographic keys. In *Proceedings of the National ComputerConference*, volume 48, page 313C317, 1979.

[3] M. Naor and A. Shamir.Visual cryptography. In *EUROCRYPT '94, Springer-Verlag Berlin*,volume LNCS 950, pages 1–12, 1995.

[4] M. Naor and B. Pinkas.Visual authentication and identification. In *Crypto '97, Springer-Verlag LNCS*, volume 1294, pages 322–336, 1997.

[5] T.H. Chen and D.S. Tsai.Owner-customer right protection mechanism using a watermarkingscheme and a watermarking protocol.

[6] P. Tuyls, T. Kevenaar, G.J. Schrijen, T. Staring, and M.V. Dijk. Security displays enablingsecure communications.

[7] S. Droste. New results on visual cryptography. In *CRYPTO '96, Springer-Verlag LNCS*,volume 1109, pages 401–415, 1996.

[8] G. Ateniese, C. Blundo, A. De Santis, and D.R. Stinson. Extended capabilities for visualcryptography. In *ACM Theoretical Computer Science*, volume 250 Issue 1-2, pages 143–161,2001.

[9] D.S. Wang, F. Yi, and X.B. Li.On general construction for extended visual cryptographyschemes.

[10] M. Nakajima and Y. Yamaguchi.Extended visual cryptography for natural images. In *WSCG Conference 2002*, pages 303–412, 2002.

[11] D. S. Tsai, T. Chenc, and G. Horng. On generating meaningful shares in visual secret sharing scheme. In *The Imaging Science Journal*, volume 56, pages 49–55, 2008.

[12] Z. Zhou, G.R. Arce, and G. Di Crescenzo.Halftone visual cryptography. In *IEEE Transactions on Image Processing*, volume 15, NO.8, pages 2441–2453, 2006.

[13] Z.M. Wang and G.R. Arce.Halftone visual cryptography through error diffusion. In *IEEEInternational Conference on Image Processing*, pages 109–112, 2006.

[14] Z.M. Wang, G.R. Arce, and G. Di Crescenzo.Halftone visual cryptography via direct binarysearch.In *EUSIPCO '06*, 2006.

[15] Z.M. Wang, G.R. Arce, and G. Di Crescenzo.Halftone visual cryptography via error diffusion. In *IEEE Transactions on Information Forensics and Security*, volume 4 No.3, pages 383–396,2009.

[16] J.O. Limb. Design of dither waveforms for quantized visual signals. In *Bell System Technology Journal*, volume 48,7, pages 2555–2582, 1969.

[17] G.J. Simmons, W.Jackson, and K. Martin.The geometry of shared secret schemes. In *Bulletin of the ICA*, pages 71–88, 1991.

[18] Zhou W. and A.C. Bovik. A universal image quality index. In *IEEE Signal Processing Letters*, volume 9(3), pages 81–84, 2002.

Author profile:

Miss. Asha S.N. [1],Pursuing M,Tech 4th sem, in(CS).

Dr.Shreedhara .K.S.M.Tech., Ph.D [2],

Smt. Anitha G. BE, ME[3],

Department of Computer Science, University B.D.T. College of Engineering, Davangere–577004, Karnataka Visvesvaraya Technological University, Belgaum,Karnataka - India.
E mail: **ashasn2007@gmail.com.**Ph: **09964379359, 09844508359, India.**