Visual Secret Sharing Scheme with Autostereogram*

Feng Yi, Daoshun Wang** and Yiqi Dai

Department of Computer Science and Technology, Tsinghua University, Beijing, 100084, China

Abstract. Visual secret sharing scheme (VSSS) is a secret sharing method which decodes the secret by using the contrast ability of the human visual system. Autostereogram is a single two dimensional (2D) image which becomes a virtual three dimensional (3D) image when viewed with proper eye convergence or divergence. Combing the two technologies via human vision, this paper presents a new visual secret sharing scheme called (k, n)-VSSS with autostereogram. In the scheme, each of the shares is an autostereogram. Stacking any k shares, the secret image is recovered visually without any equipment, but no secret information is obtained with less than k shares.

Keywords: visual secret sharing scheme; visual cryptography; autostereogram

1. Introduction

In 1979, Blakely and Shamir[1-2] independently invented a secret sharing scheme to construct robust key management scheme. A secret sharing scheme is a method of sharing a secret among a group of participants. In 1994, Naor and Shamir[3] firstly introduced visual secret sharing

---

* Supported by National Natural Science Foundation of China (No. 90304014)

** E-mail address: daoshun@mail.tsinghua.edu.cn (D.S.Wang)

scheme in Eurocrypt'94'' and constructed (k, n)-threshold visual secret sharing scheme which conceals the original data in n images called shares. The original data can be recovered from the overlap of any at least k shares through the human vision without any knowledge of cryptography or cryptographic computations. With the development of the field, Droste[4] provided a new (k, n)-VSSS algorithm and introduced a model to construct the (n, n)-combinational threshold scheme. Verheul and Van Tilborg[5] studied the (k, n)-VSSS and improved the definition from Naor and Shamir[3]. Alteniese et al.[6] proposed an extended VSSS to share a secret image. The minimum pixel expansion is obtained by using the hypergraph coloring method. Other related researches can be referred to Refs.[7-8]. Among these schemes, some groups of shares reconstruct the original secret image in security, but each share can not conceal more information without any operation.

Another interesting research based on the properties of human visual system is autostereogram (also known as single image stereogram), which is derived from stereopair or stereogram. As early as 1838, Wheatstone[9-10] discovered the stereoscopic phenomena which allows a person to see a 3D image from two 2D pictures. Julesz[11] invented the random-dot stereogram by two slightly different images. Brewster noticed the wallpaper effect which is the basis of single-image stereogram. Tyler et al.[12] designed the single image random-dot stereogram which the unaided eye could view. After that, Thimbleby[13] provided a simple and symmetric algorithm for autostereogram. Minh et al.[14] introduced a new way to detect hidden surfaces in a 3D scene and extended the algorithm to moving objects. With respect to these previous schemes, the autostereograms reveal 3D images all alone, and they are unable to hide a secret image together.

To sum up, both VSSS and autostereograms are based on the properties of the human vision. The simplicities of the secret image decryption in a VSSS and the 3D image display in an

autostereogram bring a challenging task designing a system in which each image shows a virtual 3D image and a group of images decodes a secret. Such a combinational scheme is presented in this paper. Our scheme encodes a secret image and n original grayscale images, which are n depth maps of the virtual 3D scenes revealed in the n autostereograms. The output is n images called shares that show 3D effects related to original grayscale images. Stacking any k of the n shares, the secret image is recovered, whereas no secret information appears through any less than k shares. This scheme satisfies perfect security as well.

2. Basic Model

2.1 VSSS

In a visual secret sharing scheme, the secret image consists of a collection of black and white pixels called original pixel. Each original pixel is subdivided into a collection of m black and white sub-pixels in each of the n blocks. These sub-pixels are printed in close proximity to each other so that the human visual system averages their individual black and white contributions. The collection of sub-pixels can be represented by an $n \times m$ Boolean matrix $S = [s_{ij}]$, where the element s_{ij} represents the j-th sub-pixel in the i-th share. A white sub-pixel is represented as 0, and a black sub-pixel is represented as 1. $s_{ij} = 1$ if and only if the j-th sub-pixel in the i-th block is black. The gray-level of the combined block by stacking blocks $i_1, \ldots, i_r$ is proportional to the Hamming weight (the number of ones) $H(V)$ of the OR m-vector V of the rows $i_1, \ldots, i_r$ in S. The following definition is the formal definition for the visual secret sharing scheme.

Definition 1[3] A solution to the k out of n visual secret sharing scheme consists of two collections of $n \times m$ Boolean matrices C_0 and C_1. To share a white pixel, the dealer randomly

chooses one of the matrices in C_0, and to share a black pixel, the dealer randomly chooses one of the matrices in C_1. The chosen matrix defines the color of the m sub-pixels in each one of the n blocks. The solution is considered valid if the following three conditions are met.

1. For any S in C_0, the OR V of any k of the n rows satisfies $H(V) \leq d - \alpha \times m$.
2. For any S in C_1, the OR V of any k of the n rows satisfies $H(V) \geq d$.
3. For any subset $\{i_1, \ldots, i_q\}$ of $\{1, \ldots, n\}$ with $q < k$, the two collections of $q \times m$ matrices D_t for $t \in \{0, 1\}$ obtained by restricting each $n \times m$ matrix in C_t (where $t = 0, 1$) to rows $i_1, \ldots, i_q$ are indistinguishable in the sense that they contain the same matrices with the same frequencies.

For a visual secret sharing scheme to be valid, these three conditions must be met. The first two conditions of this definition are called contrast and the third condition is called security. The pixel expansion m represents the loss in resolution from the original image to the recovered one. The relative difference α refers to the difference in weight between recovered black original pixel and recovered white original pixel. We would like m to be as small as possible and α to be as large as possible.

Example 1. The following is an example of a (2, 2)-VSSS. Encoding an original secret image (Fig.1) we obtain two shares (Fig.3 and Fig.4). Stacking the two shares, we recover the original secret image (Fig. 2).

Fig.1. Secret image

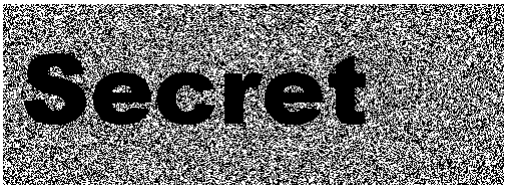


Fig.2. Recovered image

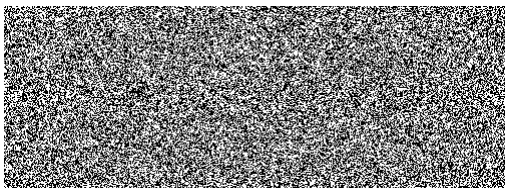


Fig.3. Share1

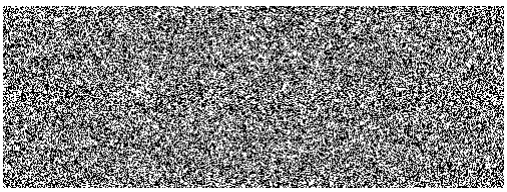


Fig.4. Share2

2.2 Autostereogram

Stereoscopic images provide a method to describe 3D objects based on the depth perception principle which is uncovered through binocular vision. Both of the eyes view two slightly different 2D images which are put together in the human brain by matching two equivalent points in the two pictures, and thus the distance of the object is perceived by the brain. There are two view techniques, cross-eyed (Fig.5) and wall-eyes (Fig.6). Actually, it is a more natural function to converge than diverge. In this paper, all autostereograms are encoded for wall-eyed viewing.

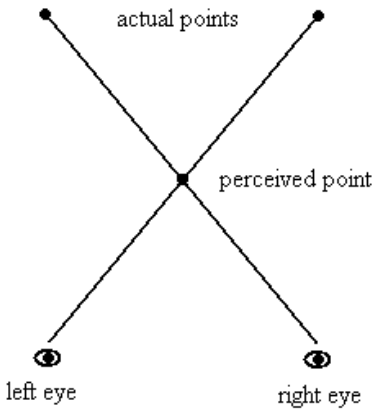


Fig.5. Cross-eyed viewing

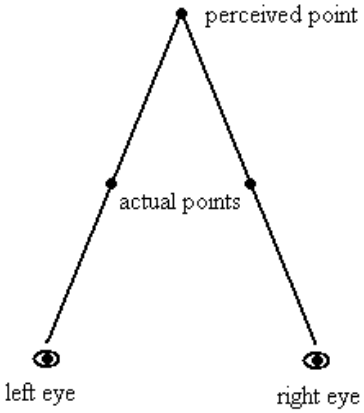


Fig.6. Wall-eyed viewing

Wallpaper effect is the basis of autostereogram. If some repeating patterns are arranged horizontally, the brain will be tricked into matching the equivalent points and perceiving a virtual plane in front of or behind the physical plane with the eyes converged or diverged. Fig.7. shows

the wallpaper effect.

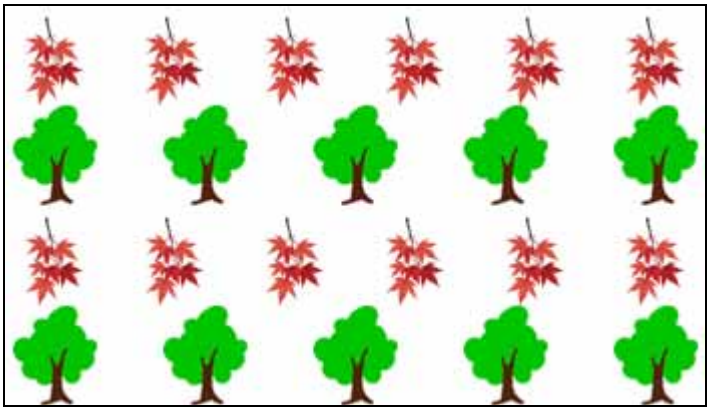


Fig.7. Wallpaper effect

Looking at these repeating patterns, we notice that the red leaves are nearer to us than the green trees, because the closer these icons are arranged horizontally, the higher they are lifted from the background plane.

Based on wallpaper effect, single image stereogram was invented. This technique is also known as autostereogram which produces a 3D effect in a 2D image. In an autostereogram, the 3D image vision depends on the space of two equivalent points. Timbleby et al.[13] analyzed the geometry form for the autostereogram, as shown in Fig 8.

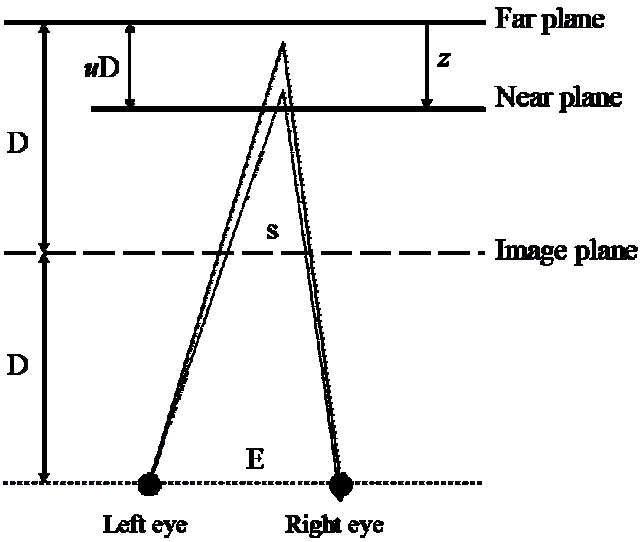


Fig 8. The geometry form

Timbleby et al.[14] provided an equation to describe the relationship between the object's depth z and the distance s of a pair of pixels that corresponds to one point in the autostereogram.

$$s = \frac{(1-uz)}{2-uz} \cdot E$$

Here, s is the stereo separation for a point, and z is a vector from the far plane to the near plane, ranging from 0 to 1. E is the distance between two pupils and u is a fixed number which is chosen to be 1/3. The equation shows that the smaller distance s produces the smaller z, and the virtual point is nearer to the eyes through wall-eyed viewing.

3. Proposed Scheme

To combine the VSSS and autostereogram, there are two possible ways. For a set of autostereograms, we need to establish the relationship among these autostereograms to conceal a secret image securely, and at the same time we must keep the 3D effect in each autostereogram. Another method is to add some 3D information into shares of a visual secret sharing scheme, and meanwhile to ensure the contrast of the recovered secret image.

Our proposed scheme realizes a (k, n)-threshold scheme in which shares are all autostereograms. The secret image is visually reconstructed by k or more shares, whereas no trace appears with less than k shares. This scheme satisfies perfect security.

The proposed scheme has pixel expansion as well. Therefore, further discussion is necessary to the distance between a pair of points that form the same virtual point. Suppose an original autostereogram with distance s_0. If an original pixel is replaced by a row vector including the original pixel and $v - 1$ random bits, the new distance s_1 between two equivalent pixels is v times larger than s_0, thus we need to reduce the distance s_1 to s_1 / v.

3.1 Construction

To construct an autostereogram, a depth map of the original 3D scene can be showed in a grayscale image in which the larger grayscale value represents the smaller distance between a pixel and its equivalent pixel to the left. 0 represents black, and 255 represents white.

The following algorithm is a construction method of (k, n)-VSSS with autostereogram.

Input:

1. An access structure (k, n) on a set P of n participants.
2. The basis matrices B_0 and B_1 of a (k, n)-VSSS with pixel expansion m
3. The color $c \in \{b, w\}$ of the pixels of the original secret image. b represents black, and w represents white.
4. The color $c_1, \ldots, c_n \in \{0, \ldots, 255\}$ of the pixels in the n grayscale images (depth maps).

Generation of the *n* shares:

1. New pixel expansion $m' = m + a$ (a is a positive integer) are arranged in m'/v rows and v columns. (In section 3.4, we will verify the minimum $a = \lceil n/(k-1) \rceil$)
2. Construct n autostereogram with distance parameters reduced to $1 / v$, based on any previous autostereogram algorithm.
3. Construct new basis matrix B'. Let $B'[i]$ be the i-th row in B'.

   The m' elements in $B'[i]$ includes all the elements in $B[i]$ and a c_i, and any other element is black. Any column in B' has at most $k - 1$ black.

Output: The matrix B'

Fig.9. The protocol to generate the shares for (k, n)-VSSS with autostereogram

There is a great difference between VSSS and VSSS with autostereogram to arrange the

subpixels in the same block. In VSSS the subpixels are arranged randomly, but in VSSS with autostereogram the pixels in the same row are constrained to the distance *s*'. For a group of the blocks at interval of *s*' in the *i*-th row, the first block to left is arranged randomly, and the other blocks are arranged in the same way. In other words, the columns in the basis matrix of the first block to left permutes randomly, and the columns in the basis matrix of the second, third, … block permutes by using the same permutation. Thus, the subpixels in the same row of an original autostereogram are still in the same row of a share.

3.2 Example

Example 2. Fig.10. and Fig. 11. are two original 3D images. Encoding them to autostereograms with distance $s_1 = 90$ and $s_2 = 90$, we got Fig.12 and Fig.13.

Fig.10. Original 3D image O_1

Fig.11. Origianl 3D image O_2

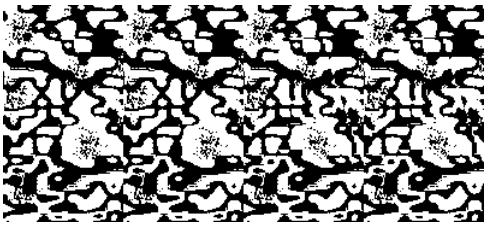


Fig.12. Autostereogram S_1

Fig.13. Autostereogram S_2

In the following, we will construct a (2, 2)-VSSS with autostereogram by using the results from example 1, and 2.

Suppose a (2, 2)-VSSS, the basis matrices are B_0 and B_1. The corresponding (2, 2)-VSSS with autostereograms has pixel expansion $m' = 4$. We arrange the four sbupixels in a 2×2 block, namely

v = 2. Assume the distance in an original autostereogram is s = 90, so we construct two new autostereograms S_1 and S_2 with new distance s' = 90/2 = 45.

For an original pixel p_0 in the secret image S_0, assume the corresponding pixels in S_1 and S_2 are p_1 and p_2. Let $D^{\{p_1,p_2\}}=\begin{pmatrix} p_1 & 1 \\ 1 & p_2 \end{pmatrix}$. Thus, $T_0^{\{p_0,p_1\}} = B_0 \circ D^{\{p_1,p_2\}}$ and $T_1^{\{p_0,p_1\}} = B_1 \circ D^{\{p_1,p_2\}}$ are basis matrices for a valid (2, 2)-VSSS with autostereograms. The experiment results are as follows.

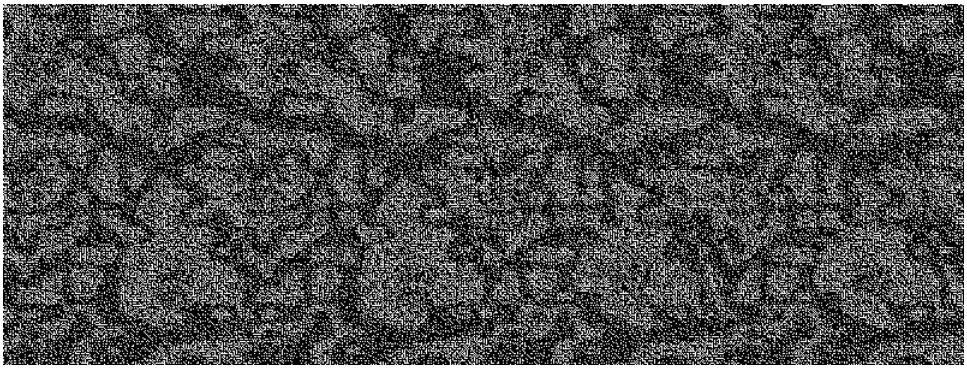


Fig.14. Share 1

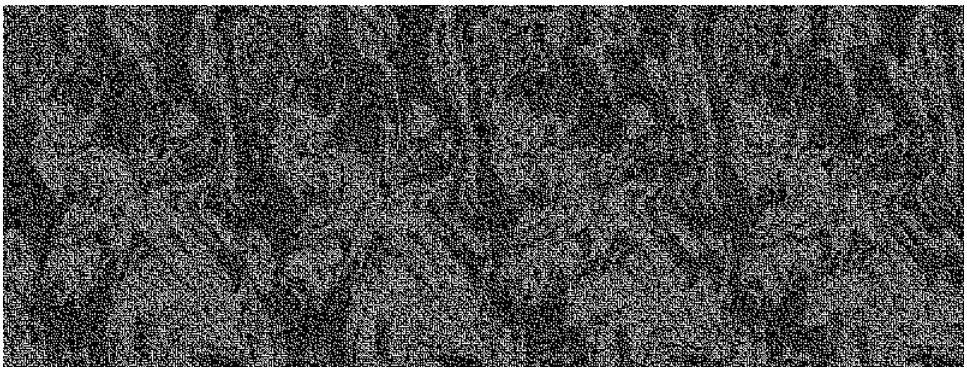


Fig. 15 Share 2

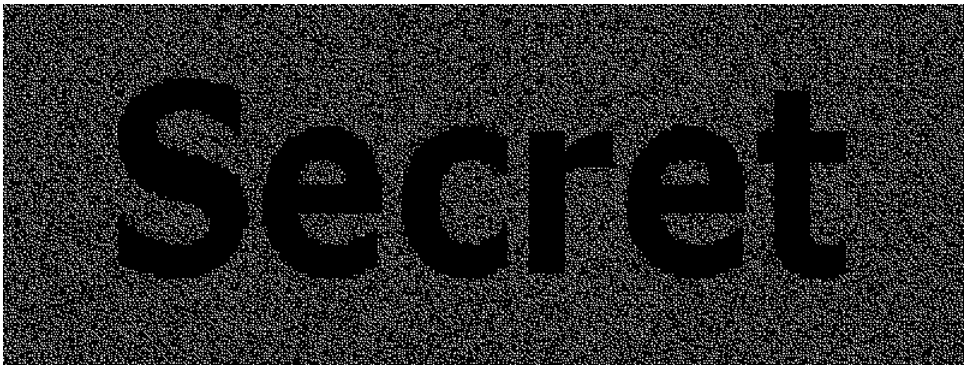


Fig.16. Share 1 and Share 2

We verify the security condition and contrast condition as follows. From the above, for a certain pair of p_1 and p_2, the Hamming weight of the i-th row in $T_0^{\{p_0,p_1\}}$ and $T_1^{\{p_0,p_1\}}$ has the same value, $i = 1, 2$. So the security condition is ensured. The contrast condition is satisfied as well. The Hamming weight of the OR of the two rows in $T_0^{\{p_0,p_1\}}$ is 3, and the Hamming weight of the OR of the two rows in $T_1^{\{p_0,p_1\}}$ is 4.

3.3 Discussion

The above construction method is implemented by combining the algorithm of autostereogram and VSSS. Now, we will provide another method to construct a (k, n)-VSSS with autostereogram. The shares of the original (k, n)-VSSS (called Scheme0 for convenience) and the new shares of the corresponding (k, n)-VSSS with autostereogram (called Scheme1 for convenience) are the same size.

The following construction is based on the n original autostereograms and the n shares of the Scheme0. Suppose these n original autostereograms and the n original shares are the same size.

Assume the pixel expansion of Scheme0 is m, and to keep the contrast of the reconstructed secret image $a - 1$ black pixels have to add to a block. Therefore, the pixel expansion of the Scheme1 is $m' = m + 1 + a - 1 = m' + a$.

Assume these m' subpixels are arranged in u rows and v columns. We compress each original autostereogram into a / m' of the original size, and each original share into m / m'. Then concatenating each original autostereogram and the corresponding original share by using the method in the section 3.2, we get the n shares of the Scheme1. An example of (2, 2)-VSSS with

autostereogram by compression is provided in the appendix.

3.4 (*k*, *n*)-VSSS with autostereogram

In Ref.[6], the authors extended the Naor and Shamir's VSSS[3] and construct an extended VSSS(EVSSS) in which each share is a meaningful image. The optimal pixel expansion is $m+.\lceil n/(k-1)\rceil$

Lemma 1[6]: Let (Γ_{Qual}, Γ_{Forb}) be an (*k*, *n*)-threshold access structure. If there exists a (Γ_{Qual}, Γ_{Forb}, *m*)-VSSS constructed using basis matrices then there exists a (Γ_{Qual}, Γ_{Forb}, $m+\lceil n/(k-1)\rceil$)-EVSSS.

Next, we will construct a (*k*, *n*)-VSSS with autostereogram. Suppose B_0 and B_1 are basis matrix of a (*k*, *n*)-VSSS. Assume *A* is a Boolean matrix called extended matrix collection which has the following three properties:

The *i*-th row in *A* has an only element to represent the pixel in the *i*-th autostereogram, $i = 1, \ldots, n$. Each column in *A* has at most $k - 1$ elements could be used to represent the pixels of the autostereograms. All the other elements in *A*are all 1's.

The next theorem proves that $T_0 = A \circ B_0$ and $T_1 = A \circ B_1$ are basis matrices of a (*k*, *n*)-VSSS with autostereograms, and the extended matrix collection *A* has the minimum pixel expansion $m_D \geq \lceil n/(k-1)\rceil$. The symbol ∘ represents the concatenation of two matrices.

Theorem 1: A (*k*, *n*)-VSSS with autostereograms can be constructed by pixel expansion $m_1 = m + m_A$ and $m_A \geq \lceil n/(k-1)\rceil$. Here, *m* is the pixel expansion of a traditional (*k*, *n*)-VSSS, and m_A is the pixel expansion of the extended matrix collection. The relative difference of the recovered secret image is $\alpha_1 = \alpha \times m / m_1$.

Proof: From the lemma1, $T_0 = D \circ B_0$ and $T_1 = D \circ B_1$ satisfies the security of the secret image. The contrast condition is verified as follows. Randomly select k rows $i_1, \ldots, i_k$. From the properties of the extended matrix collection A, the OR V_D of the k rows in A is $H(V) = m_D$. From the definition1, suppose the pixel expansion is m and the relative difference is α in a (k, n)-VSSS. The OR V_{B0} and V_{B1} of the k rows in the basis matrices B_0 and B_1 satisfies $H(V_{B0}) \le d - \alpha \times m$ and $H(V_{B1}) \ge d$. Thus we have:

$$H(V_{T0}) = \mathrm{H}(V_{B0}) + H(V_D) \le d - \alpha \times m + m_A$$

$$H(V_{T1}) = \mathrm{H}(V_{B1}) + H(V_D) \ge d + m_A$$

Therefore, the new scheme satisfies $\alpha_1 \times m_1 = H(V_{T1}) - H(V_{T0}) = \alpha \times m$, namely $\alpha_1 = \alpha \times m / m_1$.

Next, we verify the minimum pixel expansion m_D of the extended matrices colletion. From the property1 of the extended matrix collection A, The i-th row in A has an only element to represent the pixel in the i-th autostereogram, $i = 1, \ldots, n$. Thus at most n elements in A can be used to represent the pixels of autostereograms. According to the property2, each column in A has at most $k - 1$ elements could be used to represent the pixels of the autostereograms. Assume m_A be the number of columns of the extended matrix collection A. Thus $m_A \times (k - 1) \ge n$ namely $m_A \ge \lceil n/(k-1) \rceil$. ■

In the construction, the subpixels arrangement should be modified because two equivalent points in an autostereogram should be arranged horizontally and must be restricted within certain distance. One solution is to arrange the pixels in the same row of an Autostereogram on the same position in the corresponding block.

4. Conclusion

Compared with the previous schemes, our scheme implements both VSSS and autostereogram.

	autostereogram	Traditional (k, n)-VSSS	Our (k, n)-VSSS
3D effect	√	×	√
Hiding	×	√	√

Table 1. Comparison of our scheme and previous schemes.

A shortage of our scheme is that the reconstructed 3D scene in each share is not clear. One solution is 3D surface reconstruction. Each shares of our (k, n)-VSSS with autostereogram is also an autostereogram, so the previous reconstruction method can be implemented directly.

References

1. Blakley G R. Safeguarding cryptography keys. In: Proceedings AFIPS 1979 National Computer Conference, New York:USA, 1979: 313-317.
2. Shamir A, How to share a secret. *Communication of the Association for Computing Machinery*. 1979, 22(11): 612-613.
3. Naor M, Shamir A. Visual Cryptography. In: Advances in Cryptology-Eurocrypt'94, Berlin, 1995:1-12.
4. Droste S. New Results on Visual Cryptography. In: Advances in Cryptology'-CRYPTO'96, Berlin, 1996: 401-415
5. Verheul E R, Van Tilborg H C A. Constructions and Properties of k out of n Visual Secret Sharing Schemes. *Designs, Codes and Cryptography*. 1997, 11:179-196.
6. Alteniese G, Blundo C, De Santis A, Sinson D R. Extended Capabilities for Visual Cryptography. *Theoretical computer Science*. 2001, 250:143-161.

7. Ishihara T, Koga H. A Visual Secret Sharing Scheme for Color Images Based on Mean-value-Color Mixing. I*EICE Trans. Fundamentals*. 2003, E86-A(1): 194-197.

8. Cimato S, De Prisco R, De Santis A. Optimal colored threshold visual cryptography schemes, Designs. *Codes and Cryptography*. 2005, 35:311-335

9. C. Wheastone. Contributions to the physiology of vision, Part I: On some Remarkable and Hitherto Unobserved, Phenomena of Binocular Vision. *Royal Soc. Of London Philosophical Trans*. 1838, 128:371-394.

10. C. Wheastone. Contributions to the physiology of vision, Part II: On some Remarkable and Hitherto Unobserved, Phenomena of Binocular Vision (continued). *Royal Soc. Of London Philosophical Magazine and J. of Science*. 1852, 4(3):504-523.

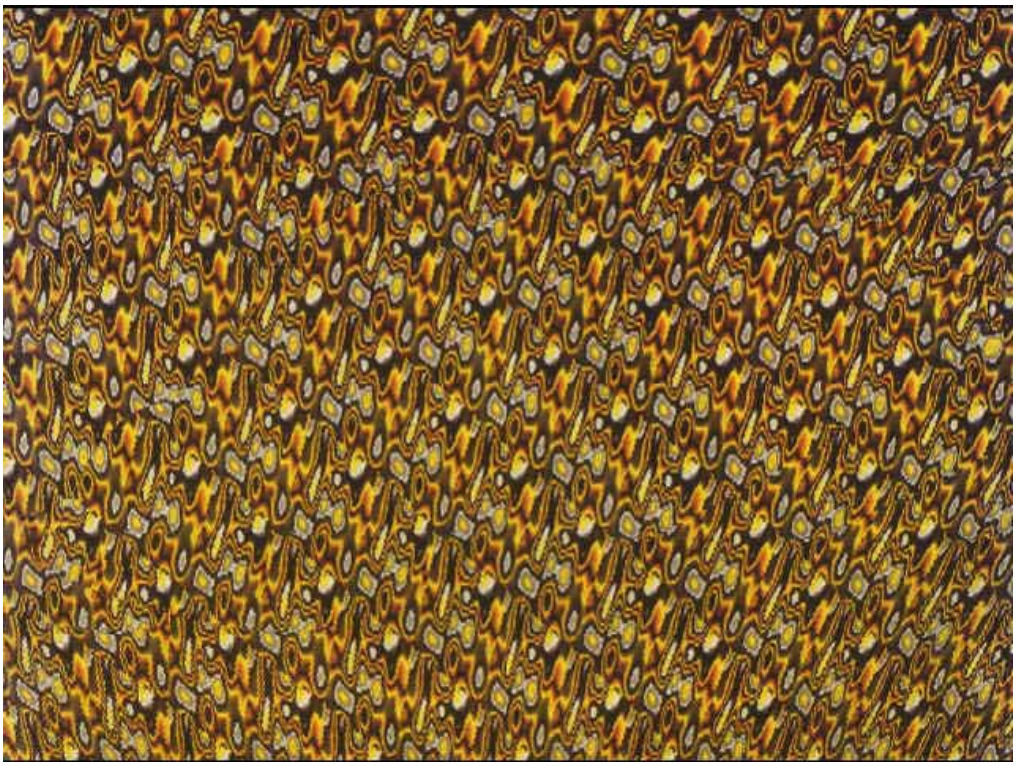
11. B. Julesz. Binocular Depth Perception of Computer Generated Patterns. *The Bell System Technical Journal*, 1960, 39: 1125-1162

12. C. W. Tyler and M. B. Clarke, The autostereogram. *SPIE Stereoscopic Displays and Applications*, 1990, 1256:182-196

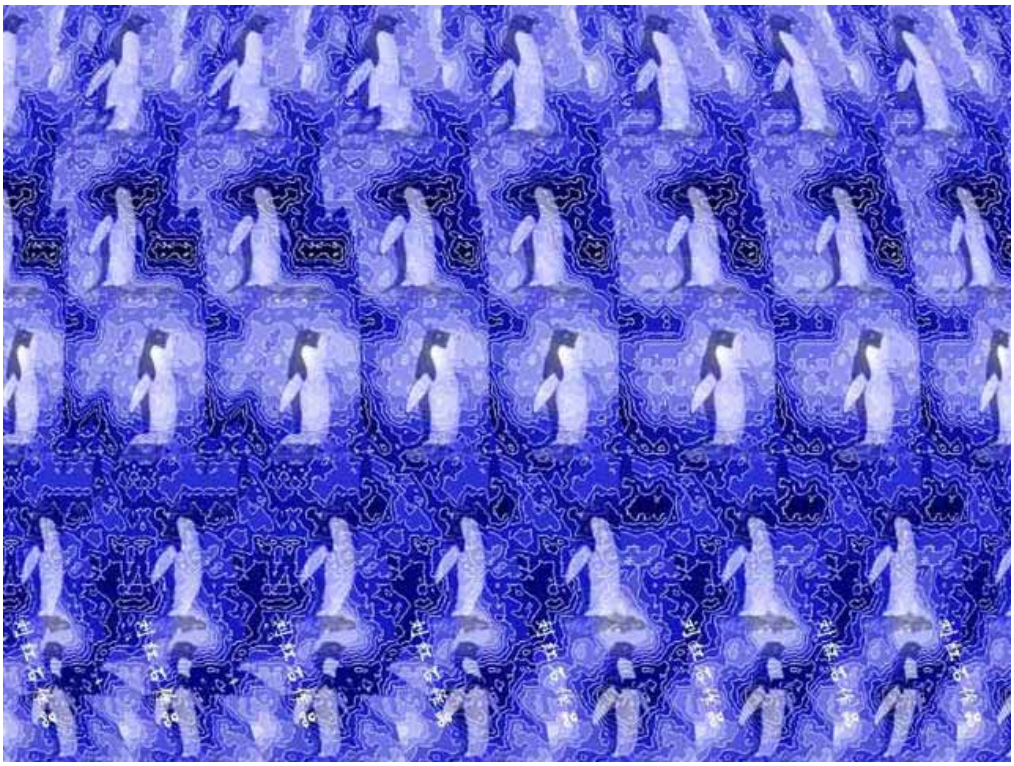
13. Harold W, Thimbleby, Stuart Inglis and Ian H. Displaying 3D images: algorithms for single-image random-dot stereograms. *Computer*. 1994, 38-48.

14. S T Minh, K Fazekas, Andras Gschwindt. The presentation of Three-Dimensional Objects with single image stereogram. *Transactions on Instrumentation and Measurement*, 2002, 51(5): 955-961

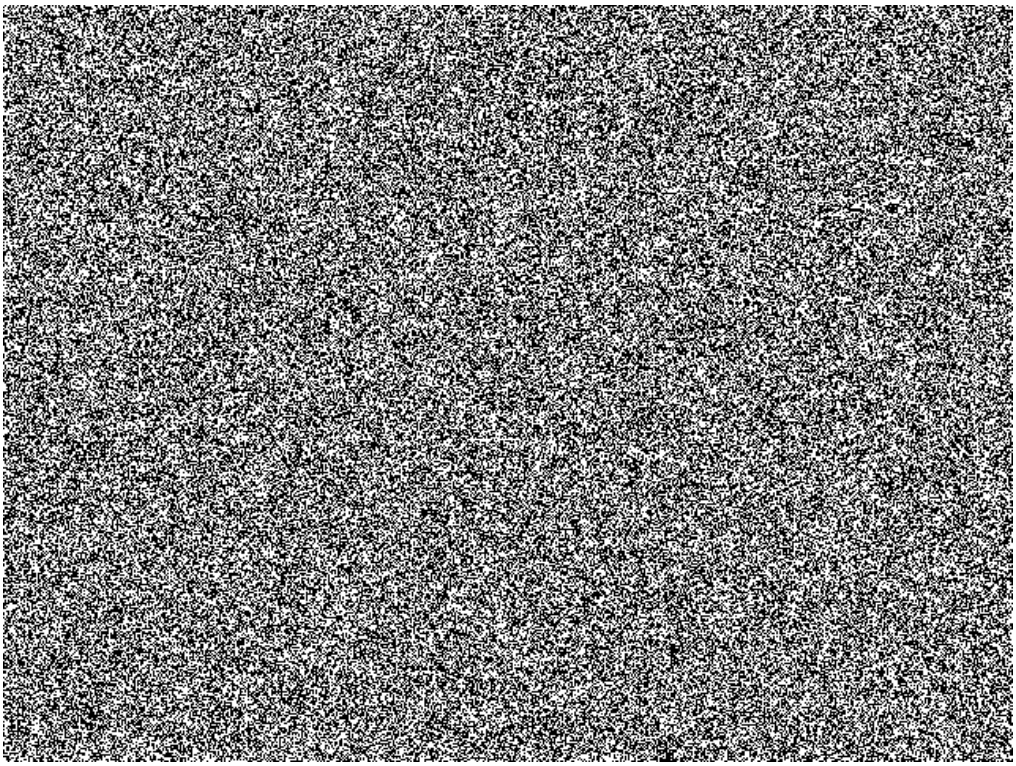
Appendix. (2, 2)-VSSS with autostereogram.



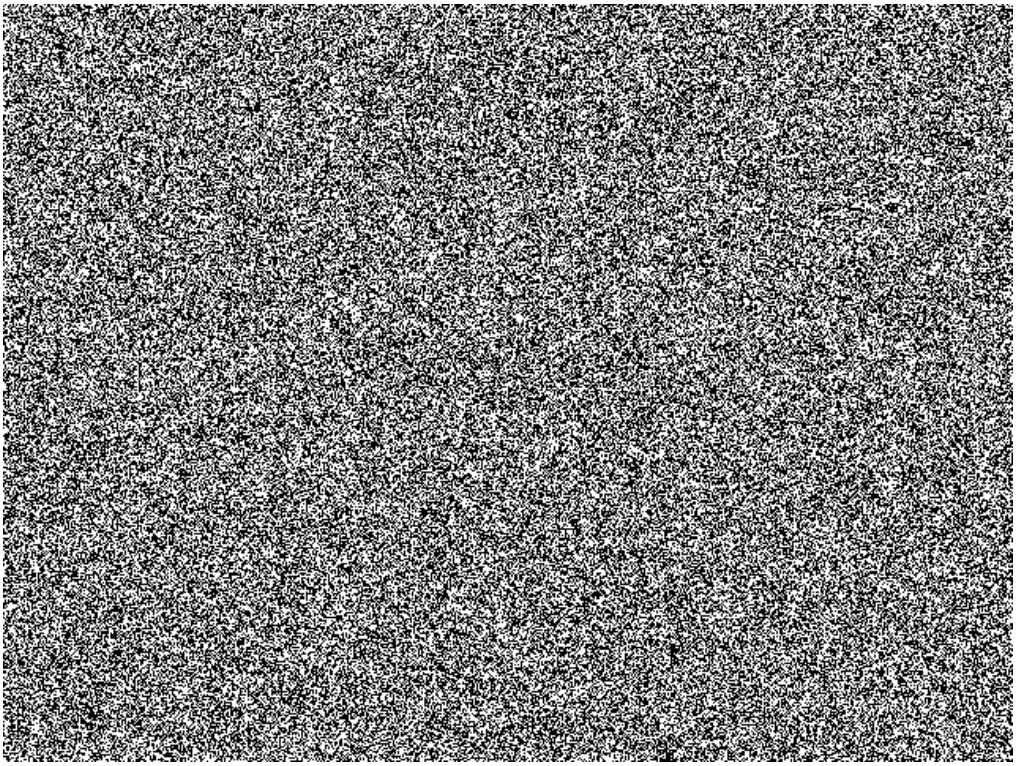
(a) Autostereogram1



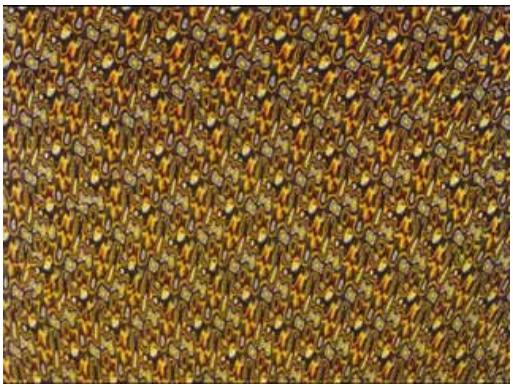
(b) Autostereogram2



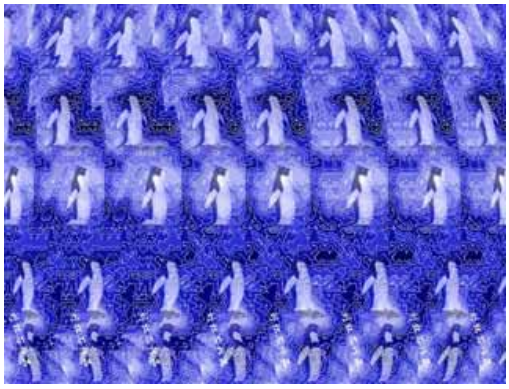
(c) Share1 of a (2, 2)-VSSS



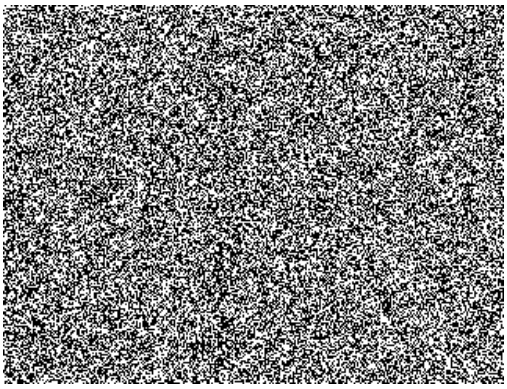
(d) Share2 of a (2, 2)-VSSS



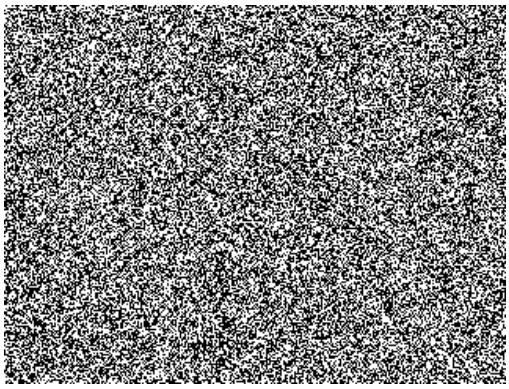
(e) Compressed autostereogram 1 (25%)



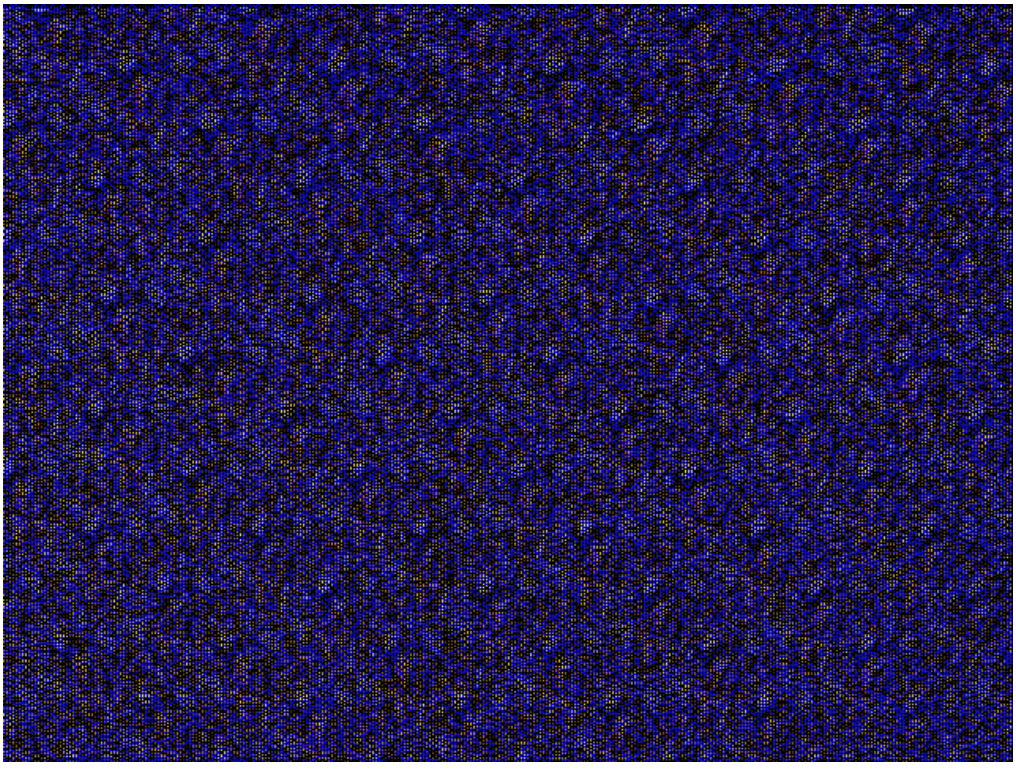
(f) Compressed autostereogram 2 (25%)



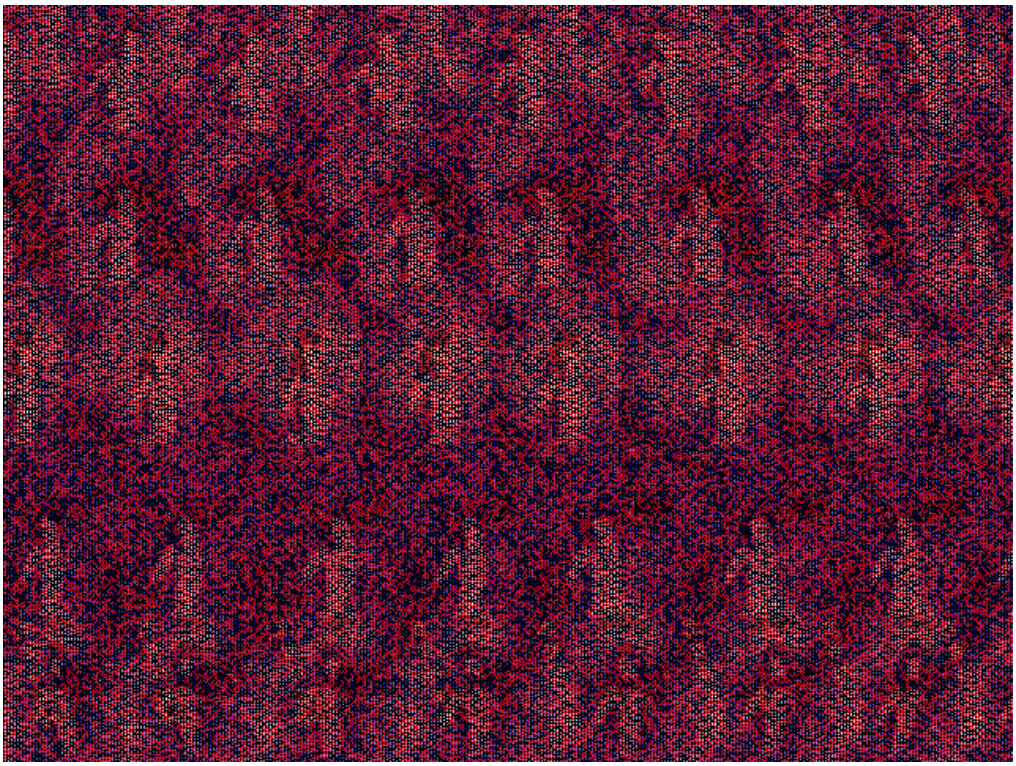
(g) Compressed share1 (25%)



(h) Compressed share2 (25%)



(i) New share1 of the corresponding (2, 2)-VSSS with autostereogram



(j) New shares2 of the corresponding (2, 2)-VSSS with autostereogram