Theoretical Computer Science 565 (2015) 30–49

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

# Visual cryptograms of random grids for threshold access structures ☆

Shyong Jian Shyu [1]

*Department of Computer Science and Information Engineering, Ming Chuan University, Guei Shan, Taoyuan 33348, Taiwan*

ARTICLE INFO

*Article history:*
Received 22 April 2014
Received in revised form 12 October 2014
Accepted 28 October 2014
Available online 4 November 2014
Communicated by G. Ausiello

*Keywords:*
Visual cryptography
Threshold visual secret sharing
Random grids
Pixel expansion

ABSTRACT

Based on a new model of visual cryptograms of random grids (VCRG), we design novel algorithms to generate a set of threshold $(k, n)$-VCRG for sharing a secret image $P$ among $n$ participants in such a way that any group of $k$ out of the $n$ encrypted transparencies reveals $P$ to our eyes when superimposed, while any group of less than $k$ transparencies obtains nothing about $P$. Just like conventional visual cryptographic schemes (VCSs), our designs require none of computing devices but merely human visual ability in the decryption process. Yet, our VCRG approach is much simpler and does not need any extra pixel expansion which is inevitable (actually $1/2^{k-1}$ for $n = k$ and even larger for $n > k$) in VCSs. The correctness of our algorithms is formally proved and experimentally demonstrated. The light contrast in our best algorithm is cautiously analyzed and shown to be as effective as that in a quality threshold VCS when $k$ shares are superimposed. With theoretic and practical interests, our VCRG model exposes new possibilities to the researches of visual secret sharing.



## 1. Introduction

To protect information from malicious interception or depredation, many elegant algorithms have been developed in traditional cryptography. Modern technologies such as data hiding, watermark, steganography, etc., may be other choices for safeguarding information. These approaches require electronic computing devices to provide the computations in both of the encryption and decryption processes. In general, the higher the level of secrecy is demanded, the more the computations are needed. The common vulnerability of these approaches would be the damage of the ciphertext (or key) itself by malicious intruders or improper storage management such as the humidity or exceptional weather disasters (say flood, earthquake, etc.). Once the ciphertext (or key) has been physically ruined, the secret cannot be recovered.

*Secret sharing* is another choice for protecting information. In a *k out of n* (or $(k, n)$) secret sharing scheme, a secret is encoded into $n$ parts distributed to $n$ participants such that any group of $k$ participants can decode the secret using their parts, while that of less than $k$ ones cannot. The secret is thus *shared* among the $n$ participants and tolerant to a loss of $n-k$ parts. This relieves the vulnerability of the aforementioned approaches to a certain degree. Still, the electronic computations are inevitable in both encoding and decoding.

☆ This research was supported in part by the Ministry of Science and Technology, Taiwan, under Grants MOST 102-2221-E-130-005 and 103-2221-E-130-002-MY3.

*E-mail addresses:* sjshyu@mail.mcu.edu.tw, sjshyu@gmail.com.

[1] Tel.: +886 3 3507001x3322; fax: +886 3 3593874.

http://dx.doi.org/10.1016/j.tcs.2014.10.048
0304-3975/

In some circumstances where the cost of computations may not be affordable, the decoding time should be instantly done in a constant time, or the recognition of the secret shape/pattern is sensitive or meaningful only to the human perception, to name a few, these computation-based algorithms become no longer appropriate.

*Visual cryptography* proposed by Naor and Shamir at Eurocrypt'94 [1] is a visual version of secret sharing. A secret image can be shared among several participants and the decoding process is done by human visual ability so that no computation is required. Specifically, a $k$ out of $n$ *threshold visual cryptographic scheme* ($(k,n)$-VCS) is able to encrypt a binary secret image $P$ into $n$ ($\geq 2$) shares printed as transparencies such that only when $k$ ($\leq n$) transparencies are superimposed altogether can $P$ be revealed to our eyes, while any group of less than $k$ transparencies receives nothing about $P$. Their $(k,n)$-VCS integrates the ability of human visual perception into the decryption process to absolve the computation requirement in a perfectly secure way.

With such an attractive feature that no computation is required but only human visual perception in decoding, visual cryptography has drawn much attention since then. Essentially, a $(k,n)$-VCS, based upon the definition in [1], expands each pixel $p$ in $P$ into $n$ shares of $m$ sub-pixels each (represented as an $n \times m$ *basis matrix* $B^p$ for $p \in \{0,1\}$) to diffuse and disguise $p$ which would only be visually perceivable with *a loss of contrast* by stacking $k$ (or more) transparencies. Therefore, (1) the *pixel expansion* ($m$) of the basis matrices, i.e. the number of the sub-pixels to encode each pixel, (2) the *relative contrast* between the reconstructed white and black pixels are the most critical measurements to evaluate the effectiveness of a $(k,n)$-VCS. It is expected that the pixel expansion of a VCS could be as smaller as possible (to avoid a large size of the encoded shares), while the contrast as higher as possible (to ease our visual recognition of the reconstructed result).

The general construction of a $(k,n)$-VCS was first introduced by Naor and Shamir [1]. Based upon their elegant $(k,k)$-VCS (in which the pixel expansion $2^{k-1}$ has been proved to be optimal [1]), they incorporated the skills of *k-wise independent hash functions* or *small-bias probability spaces* to prove the existence of a $(k,n)$ scheme with pixel expansion $m_{\mathrm{VCS}}^{(k,n)} = n^k \times 2^{k-1}$ or $\log n \times 2^{O(k \log k)}$, respectively. Ateniese et al. [2] presented a construction for $(k,n)$-VCSs by using *perfect hashing*. Their scheme takes $m_{\mathrm{VCS}}^{(k,n)} = l \times 2^{k-1}$ where $l$ is about $O((\log n)^{\log(C(k,2)+1)})$ or $O(ke^k)\log n$ depending on the perfect hashing function adopted. Droste [3] deliberately devised a constructive algorithm with a smaller pixel expansion than the previous results. Kotoh and Imai [4] formulated the relations between the basis matrices and the requirements of a $(k,n)$-VCS as a linear system and built the basis matrices by solving the linear system. Their approach results in the same pixel expansion as Droste's scheme. By adopting sophisticated skills of linear programming, the optimum pixel expansion of a $(2,n)$-VCS was shown by Eisen and Stinson [5] and that of a general $(k,n)$-VCS was explored by Shyu and Chen [6].

On the basis of $(k,n)$-VCSs, more interesting subjects such as the constructions, bounds or contrasts [1,7–9,12], *general access structures* (GAS) [2,7], *extended capabilities* [10], *region incrementing* [11], or realizations for color images [12–15], and so on have been developed in the circuit of visual secret sharing. The role of an effective $(k,n)$-VCS is undoubtedly substantial.

The concept of *random grids* was initially introduced in [16] for encrypting a secret image. It may be the first successful incorporation of human visual intelligence and cryptography. Shyu gave a formal definition to the *visual cryptograms of random grids* (VCRG) to make VCRG applicable in visual secret sharing and devised algorithms for $(2,2)$-VCRG [17], $(k,k)$-VCRG [18], VCRG for sharing multiple secrets [19] and VCRG for GAS [20]. Similar works by other research groups could also be found in [21–23]. The most essential advantage of applying VCRG lies in that neither extra pixel expansion nor basis matrices are needed.

Our goals in this paper include (1) to develop more effective algorithms for producing $(k,n)$-VCRG without any extra pixel expansion nor any basis matrix, and (2) to compare the performances of the proposed $(k,n)$-VCRGs. As compared to those $(k,n)$-VCSs which take pixel expansions no less than $2^{k-1}$ and are based upon sophisticated mathematical knowledge, our algorithms are much simpler, not needing any basis matrices and $m_{\mathrm{VCRG}} = 1$ (so that the encoded shares are of the same size as the original secret).

The rest of the paper is organized as follows. Section 2 introduces the definition of a conventional $(k,n)$-VCS, illustrates the basic concepts of VCS and VCRG, and clarifies the advantages/disadvantages between them. Section 3 establishes the foundation of VCRG and presents the designs and analyses of the proposed $(k,n)$-VCRG algorithms. The experimental results and analytic discussions are given in Section 4. Concluding remarks are drawn in Section 5.

## 2. VCS vs. VCRG

### 2.1. Definition of $(k,n)$-VCS

Let $H(V)$ denote the Hamming weight of a binary vector $V$. The definition of a $(k,n)$-VCS proposed by Naor and Shamir [1] with parameters $k$, $n$, $m$, $d$ and $\alpha$ is as follows where $2 \leq k \leq n$, $1 \leq d \leq m$ and $0 < \alpha < 1$.

**Definition 1.** 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 $n$ transparencies. 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 $H(V) \leq d - \alpha \cdot m$.
2. For any $S$ in $C_1$, the "or" $V$ of any $k$ of the $n$ rows satisfies $H(V) \geq d$.