Sharing a Verifiable Secret Image using Forward Error Correction Code for Halftone Image

Chun-Yu Chen[1], Jyun-Jie Wang[2], Chi-Yuan Lin[1], Chuin-Mu Wang[1],Cheng-Yi Yu[1]

[1]*Department of computer Science and Information Engineering Nation Chin-Yi University of Technology 35,chung-Shan rd.,Taichung 41101 Taiwan, R.O.C.*

[2]*Graduate Institute of Communication Engineering and Dept. of Electrical Engineering National Chung Hsing University 250,kuo kuang Rd., Taichung 402, Taiwan*

grrmin@gmail.com;fractals_jie@pchome.com.tw;chiyuan@ncut.edu.tw

Abstract—**A novel verifiable secret sharing method for Verifiable secret sharing (VSS) in halftone image based on linear block code with a parity check matrix is proposed. The proposed method, which not only verifies a secret image but also introduces multiple shadows for multiple users. The proposed method adopts forward error correction code (FEC) strategy based on property of linear block codes. There are three advantages for the proposed method: (1)the proposed scheme is capable of offering multiple shadows, (2) The proposed scheme is of low computational cost and (3)The novel VSS allows users to verify the shadows or enhance the robustness of original shadows. Experimental results show that the proposed scheme is capable of efficiently verifying a secret image from a variety of users. Moreover, the VSS process multiple shadows without pixel expansion. The experimental results show that the novel VSS scheme is low computational complexity.**

Keywords— **Hamming code, Visual secret sharing, halftone image, Error diffusion.**

1. INTRODUCTION

As the public network communication progresses significantly, a large amount of data must be transmitted in a number of reliable ways, one of which is the so called cipher key management technique. Verifiable secret sharing is a important method for cipher key management. According to the importance, the VSS system produce distinct cipher key. In order to has better security for cipher key management, the main cipher key may be divided into several shadows. Thus, the cipher key management system will consider the tradeoff between security and complexity system.

A secret sharing scheme with (M, M) threshold offer N participants to obtain the shadows. Participants can share the secret data together while the shadow threshold M is achieved. There- fore, the number of participants is only greater than M and the secret message is reconstruct. First presented by Blakley[1] and Shamir[2] in 1979, this method employ prime and polynomial from Lagrange's interpolation to achieve share secret scheme. The proposed method by Blakley and Shamir offer a secret number to participants. In 1995, Naor and Shamir[3] further extended the secret sharing scheme to a secret image, called a visual secret sharing scheme. VSS have been presented in [1,3,4,5,6,7,8]. There is a disadvantage among [9,10,11]. Although these methods is simple, they bring to a problem of pixel expansion. In this paper, we employ forward error correcting code to improve this problem. We propose the novel method which is a low complexity and a (M, M) VSS system based on FEC strategy, called forward error correction sharing code (FECSC). This can produce several shadows (codewords) from forward error correction code and $M-1$ shadows is of hiding or correcting capacity. The proposed system is capable of sharing a secret message or correcting some error patterns. The novel method utilizing the characteristic of forward error correction code and therefore the novel VSS system is simple and low computational complexity. For the security season, we employ random linear block codes to construct the VSS system. In order to enhance the security, the length of random linear block codeword may be increased. In this paper, we also construct the VSS system by convolution codes. In random linear block codes case, the standard array consist of a variety of uniform weight coset leader to cover the original message.

The rest of this paper is organized as follows. In Section Ⅱ, we briefly describe the related

[1]This work was supported by Grant NSC-98-2221-E-005-037.

works. In Section Ⅲ, we illustrate the key technology and propose the novel secret sharing method. In Section Ⅳ, shows our experiment and result. Finally, We provide some conclusion and discussion in Section Ⅴ.

2. RELATED WORKS

2.1. Standard array and syndrome

Standard array is considered to be one of efficient classified techniques based on linear block codes. The basic ideal of standard array is that a space F_2^n is partitioned into 2^k disjoint subsets $D_1, \cdots, D_2^k$ based on linear block code $\mathrm{C} = \{c_1, \cdots, C_2^k\}$. The standard array is constructed as follows. First, the codeword c_i of C in a row and the all-zeros codeword $(0, \cdots, 0)$ as the first element. From the remaining $2^n - 2^k$ vectors, we choose a minimum weight vector e_1 and place it under the all-zeros codeword. Now, we form a second row by adding e_1 to each codeword, $\mathrm{C} + e_1$, and placing the sum $\mathrm{C} + e_1$ under C. Having completed the second row, we choose a minimum weight vector e_2 from the remaining vectors and place it under C. Then, we form a third row by adding e_2 to each codeword C_i. This process is performed until we have used all the vector in F_2^n. These e_i vectors is called coset leader and the syndrome is defined as $\mathrm{H}e_i^T$.If the received vector y is found in the subset D_i, y is decoded into C_i.

2.2. Matrix Embedding

In this subsection, we illustrate the a efficient strategy for binary data embedding. For example, a (7,4) hamming code employs a parity check matrix H, defined as

$$H = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

In the case of an ordinary $(2^m - 1, 2^m - 1 - \mathrm{m}, 3)$ hamming code, where the integer $m \geq 3$, the embedding distortion as well as the embedding capacity is 1/7 and 3, respectively. A distortion of $1/(2^m - 1)$ change/bit along with an embedding capacity of m bit can thus be gained. Using H to estimate the host vector syndrome s_u, a hamming code discovers the difference s_x between s_u and the logo vector, s_l, intended for embedding. Finally, a column vector, identical to s_x, of H is located and the corresponding host vector position is altered accordingly. This is referred to as the parity check code algorithm. Well extended, an arbitrary (n, k) linear code can be described by H, with a (7,4) hamming code as a special case. Ultimately, any algorithm, employing a parity check equation to perform embedding, can all be characterized with H.

3. FORWARD ERROR CORRECTION SHARING CODE

In the section, we proposed the verifiable secret sharing system which employ matrix embedding to hide the binary secret message. Assume that each participant holds a secret image, called a shadow. The proposed system is not only capable of producing multiple shadows but also verify whether shadows is legal or not. In our scheme, we adopt the property of linear block codes to process the multiple shadows. Assume that there are M multiple shadows is construct by the proposed system. We can assure that there are $M - 1$ shadows can be verified by secret logo. The rest of the shadows is only a pure shadow without verifying logo.

The secret sharing scheme and verifying logo scheme is called as forward error correction sharing code, FECSC, system. The FECSC system is illustrated in Fig. 1.

Fig. 1, briefly is divided into four parts: (1) Codeword separate scheme, (2) hiding the verifiable logo scheme and (3) hiding verifiable logo and (4) reveal the cipher image scheme.

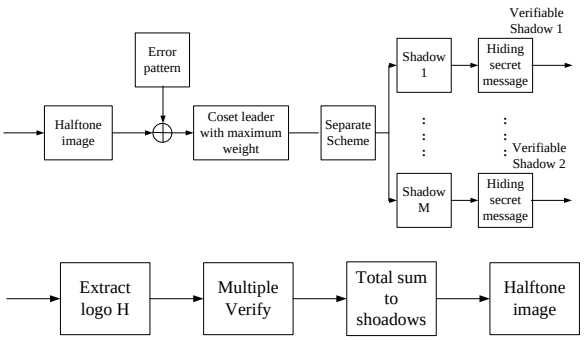


Fig. 1 Block diagram of FECSC scheme.

3.1. Hiding binary verifiable logo by matrix embedding

Given a halftone image and a secret message intended for embedding, the syndrome of the halftone image must be firstly estimated and then added to that of the logo message as a way to acquire a toggle syndrome. Ultimately, the coset

leader, corresponding to the toggle syndrome, can be found using the maximal likelihood (ML) decoding. The coset leader is then added to the halftone image as a way to yield a closest vector, into which a secret message is embedded. This is illustrated Fig. 2. As follows.

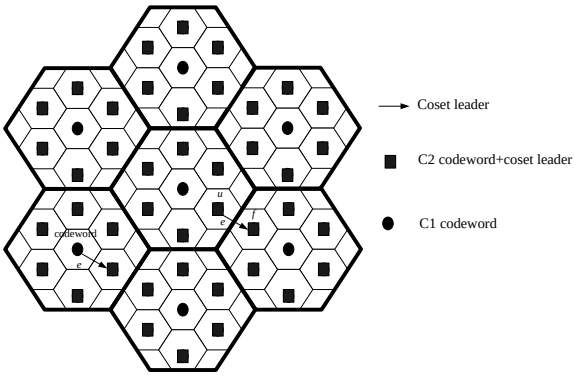


Fig. 2. ML algorithm expression

A (n,k) linear block code C can be characterized with a parity check matrix H of size $(n,k)\times n$. Furthermore, the set composed of all the sequences r, corresponding to the identical s, is referred to as the coset of the code C , defined as

$$C^s = \{r|H_r = s\} = \{\, c + e|c \in C\}$$

where e denotes the coset leader in the standard array. s can be derived through H from an arbitrary sequence r, and e can be expressed, in terms of a ML decoding function, as

$$e = f(H_r) = f(s)$$

Where $f(\cdot)$ represents the linear codes decoding function. Determined through ML decoding, the coset leader e is added to r as a means to recover the code C, that is closest to the sequence r. There exists a halftone image corresponding to an arbitrary sequence u of length n bits within the coset C^u of the standard array. The syndrome $s_u = Hu^T$ corresponding to C^u is referred to as the halftone image syndrome. Referred to as the secret message, a known binary sequence s_l of length $n-k$ bits is intended for embedding. It is known with ease that the coset leader e_{opt} must be located within a set C^u ahead before a sequence, closet to u, with syndrome s_l, is discovered. Then the syndrome s_x is determined by the addition of secret message sequences s_l to s_u . From the view point of decoding, the coset leader e_{opt} can be discovered through ML decoding, expressed as

$$e_{opt} = f_{opt}(s_u + s_x) = f_{opt}(s_x)$$

Suppose that a sequence $x \in \mathrm{C}^x$ exists, and represent a coset of the code. It is intended to seek with the minimal weighting, x that is, $x = e_{opt}$, which is expressed as

$$e_{opt} = \arg \min_{x\in C^x} w_H(x)$$

Once discovered, the coset leader e_{opt} is added to the halftone image as u.

$$l' = u + e_{opt}$$

Essentially, l' is the sequence, closet to the sequence u within F_2^n dimensional space, and contains the secret message sequence s_l . In steganography, employ the ML algorithm to find the optimal fidelity, coset leader, and to embed some logo message. The purpose of VSS system is opposite. The purpose of VSS briefly shade the original image to avoid revealing, hence we shall choose the coset leader which the weight is closet to half of codeword length as

$$e_h = arg_{w_{H(x)}}$$

Although the weight of codeword is large, the syndrome corresponding to arbitrary vector is identical.

3.2. Linear block code for sharing scheme

In this section, We further describe FECSC structure to improve the original article [12]. Here, we propose a strategy of codeword separation to produce new shadows. First, a standard array of random linear block code is constructed as Fig. 3. The standard array is not the same as conventional that. The distinct standard array consist of coset leader which weight is equal to $\lfloor n/2 \rfloor$. Instead of using minimum weight is equal to half length of codeword, as coset leader e in the coset C^e. Thus, we shall shade the original halftone image as shadow and the shadow is more security.

Assume arbitrary vector u in above standard array given by

$$u = e_i + C_j$$

Where e_i is the coset leader corresponding to coset C^e and C_j is a codeword of linear block in C. The e_i and C_j vector is employed as two shadows s_1 and s_2 , respectively. According to the property of linear block, the C_j is linear combination by two distinct codeword C_j' and C_j'' as

$$C_j = C_j' + C_j''$$

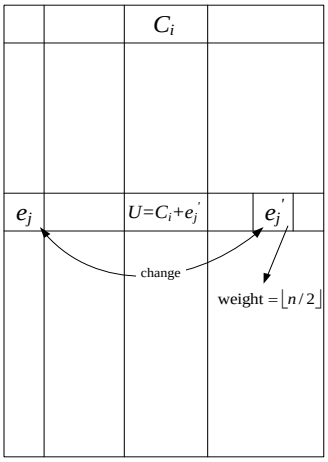


Fig. 3. Stardand array for sharing scheme.

We can use iterative above formula to offer new codeword of linear combination. More shadows can be produce as long as the formula is performed continuously. Finally, there are $2^L + 1$, where L is iterative time, shadows $C_{L,i}$ is produced as

$$C_j = \sum_{i=1}^{L} \sum_{j=1}^{2^i} C_{i,j},$$

Where $C_{i,j} \in C$.

The separation strategy of codeword in section [12] is also capable of applying to broadcast channel besides point to point channel. We review the separation strategy as $C_j = C_j' + C_j''$. The codeword C_j is constant while the formula is applied to broadcast channel. The codeword C_j'' is applied to broadcast channel. The codeword C_j'. We compare the point to point channel with broadcast channel as Fig. 4.

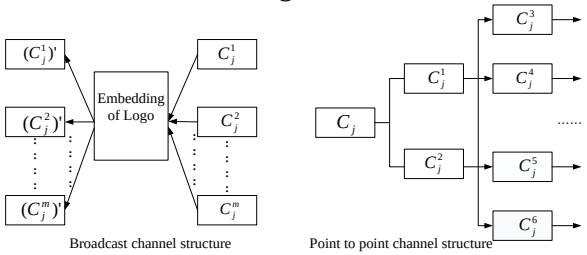


Fig. 4. Application for broadcast system.

Based on separation strategy of codeword, FECSC system is capable of applying to a variety of field.

Generally, the length of linear block codes is short. In order to enhance the security of FECSC scheme, we attempt to employ the linear block code with large length. Although that can bring more security, corresponding to standard array is difficult to constructed. Thus, another candidate is convolutional codes. A convolutional codes perform large length sequence in a trellis. Hence, the codeword correspond to convolutional code is large length and security.

Finally, the FECSC scheme is performed algorithm as follows:

Algorithm FECSC scheme for halftone image

1. Read the halftone image u and calculate error pattern *e*.
$$e = f(u)$$

2. Choose a half weight e_h to be coset.

3. Employ the separate strategy to find the multiple shadows S_i

4.Extract and perform the multiple verify$S_l = HS_i$.

5. Total sum to shadows $U = \sum S_i + e_h$.

4. SIMULATION RESULTS

In the section, we illustrate experimental result of security and computational complexity.

1) Security

In order to measure the security of proposed system , we employ number of pixels change rate(NPCR). NPCR is defined as

$$\mathrm{NPCR}(\mathrm{C}_1, \mathrm{C}_2) = \frac{1}{\mathrm{xy}} \sum_{\mathrm{i}=1}^{\mathrm{x}} \sum_{\mathrm{j}=1}^{\mathrm{y}} \mathrm{W}(\mathrm{C}_1, \mathrm{C}_2),$$

where $\mathrm{W}(\cdot)$ is the hamming distance function. According to[12], the expected NPCR value is approximate to $(1 - 2^{-B} \times 100\%)$, where B is the number of bit from presenting a pixel of various shadows. Here, the experiment is performed by a variety of random linear block code. The experimental result about approximate NPCR as TABLE 1 and TABLE 2 and shadows set for halftone image as TABLE 4 and 5.

TABLE 1

Chang et al. [12]				
Image	Lena	Airplane	Sailboat	Tiffany
(7,4)	67.43	79.08	80.46	94.56

TABLE 2

The proposed scheme			
Image	Lena	Airplane	Sailboat
(7,4)	74.22	77.23	73.61
(10,4)	74.87	74.93	74.41
(10,8)	74.49	77.75	74.57
(12,4)	74.64	75.70	73.93
(12,8)	74.36	75.80	74.79
(16,4)	73.29	75.55	75.04
(16,8)	75.01	75.04	74.87
(16,12)	74.96	75.61	74.89

The proposed scheme			
Image	Baboon	Goldhill	Sail
(7,4)	74.99	73.87	71.44
(10,4)	73.98	73.35	72.67
(10,8)	75.07	74.02	74.01
(12,4)	73.72	73.13	72.28
(12,8)	74.98	74.55	74.87
(16,4)	74.53	73.68	73.26
(16,8)	75.06	74.94	75.10
(16,12)	75.02	74.76	74.77

When we intend to offer correcting capacity without embedding verifiable logo, the shadows is straight employed.

2) Computational complexity

As follows, the algorithms stated above are simulated on the operational time in TABLE 3. The programs are developed in MATLAB R2007a, and executed and Intel(R) CORE 2 CPU 2.93G on a computer with 2G DRAM, and the training samples halftone image and secret message are selected randomly.

TABLE 3

The proposed scheme vs. Chang et al. in second				
image	shadows	Logo size	Chang et al.	FECSC
Lena	2	335x335	91.12s	6.57s
Airplane	2	335x335	90.74s	6.47s
Sailboat	2	335x335	89.38s	6.50s
Baboon	2	335x335	90.10s	6.46s
Goldhill	2	335x335	91.33s	6.48s
Sail	2	335x335	90.44s	6.56s

5. CONCLUSIONS

In this paper, the FECSC scheme is proposed to further improve conventional verifiable secret sharing scheme. In order to construct the FECSC scheme, we employ codeword separation method to achieve multiple shadows. The FECSC scheme not only verifies secret logo but also corrects the shadow which suffer from channel attack. Moreover, the FECSC scheme allows multiple shadows which is capable of verifying the secret logo. Because of separation method, the proposed FECSC scheme is low complexity than conventional VSS scheme. The proposed scheme is also without problem of pixel expansion. Experimental result show that a variety of test image is performed by proposed algorithm. The results illustrate that the original image is reconstructed by performing sum operation and the secret logo is completely extracted.

REFERENCES

[1] G.R Blakley, “Safeguarding cryptographic key”, in: proceedings of the National Computer Conference, American Federation of Information Processing Societies, June 1979, pp. 313-317

[2] A. Shamir, “How to share a secret” Communication of ACM 22(11)(1979)612-613

[3] M. Naor, A. Shamir, “visual Cryptography”, Advances in Cryptology-Eurocypt’94 , in: Lecture Notes in computer Science, Vol.950. 1995, pp. 1-12

[4] A. Adhikari, A.Sikdar, “A New (2,n)-visual Threshold Scheme for Color Image”, in:INDOCRYPT 2003, Lecture Notes in Computer Science, vol.2904,2003,pp. 148-161

[5] C. Blude, A, De Santis, M. Naor, “Visual Cryptography for grey level image”, Information Processing Letters 27(2000)255-29.

[6] Y.F Chen, Y.K. Chan, C.C. Huang, M.H. Tsai, Y.P. Chu, "Amultiple-level visual secret-sharing scheme without image sizeexpansion", {\it Information Sciences} 177(21)(2007)4696-4710.

[7] G.Horng, T.Chen,D.Tasi,Cheating in visualcryptography,Designs,Codes and Cryptographty 38 (2006) 219-236

[8] R.Ito, H.Kuwakado,H.Tanaka,Image size invariant visual cryptography, IEICE Transactions on Fundamentals E 82-A (10)(1999) 2172-2177

[9] S.Cimato, R.De Prisco, A.De Santis, Probabilistic visual Cryptography schemes, The computer Jounal 49(1)(2006)97-107

[10] D.Wang, L.Zhang, N.Ma, X.Li , Two secret sharing schemes based on Boolean operations, Pattern Recognition 40 (2007)2776-2785

[11] C.N.Yang, New visual secret sharing schemes using probabilistic method, Pattern Recognition Letters 25(4) (2004) 481-494

[12] C.C. Chang, C.C.Lin, T.H.N.Le, H.B.Le, Sharing a verifiable secret image using two shadows, Pattern Recognition, Volume 42, Issue 11, November (2009)3097-3114

TABLE 4

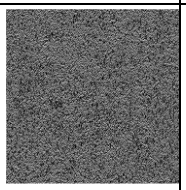
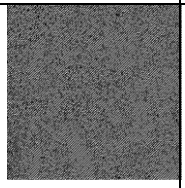
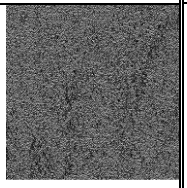
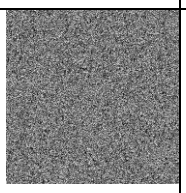
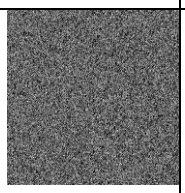
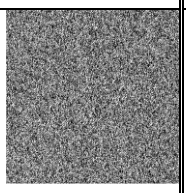
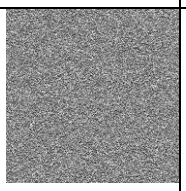
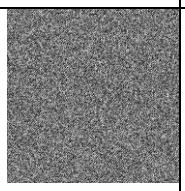
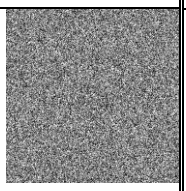
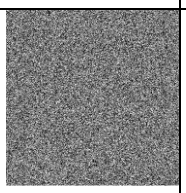
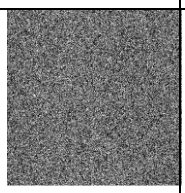
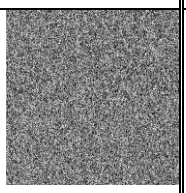
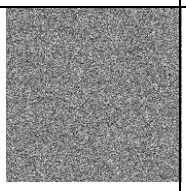
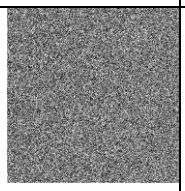
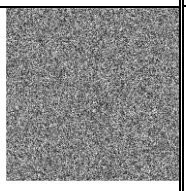
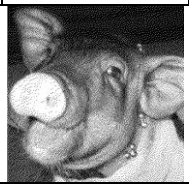
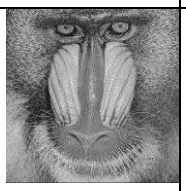
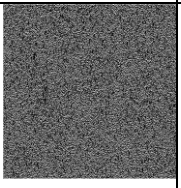
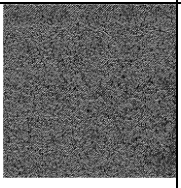
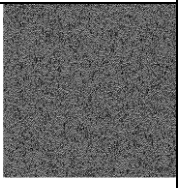
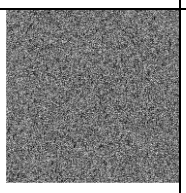
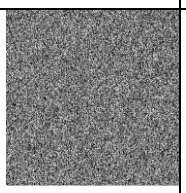
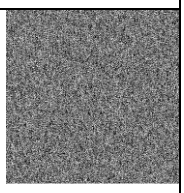
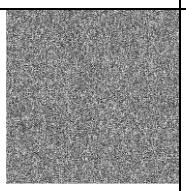
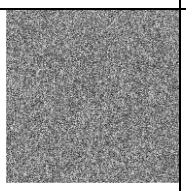
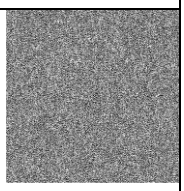
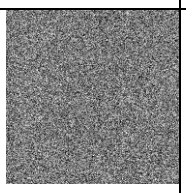
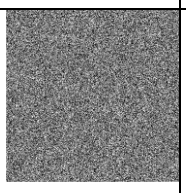
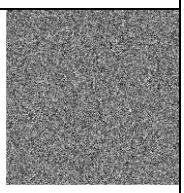
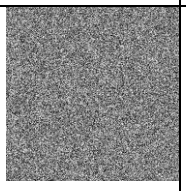
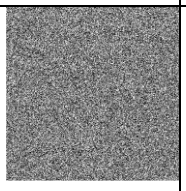
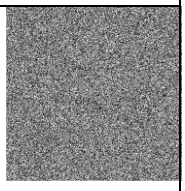
Cover image with the proposed scheme			
	Airplane	**Tiffany**	**Lena**
Original image			
Shadow1			
Shadow2			
Sjadpw3			
Embedding of shadow2			
Embedding of shadow3			
Logo			

TABLE 5

Cover image with the proposed scheme 2			
	Baboon	**Goldhill**	**Sail**
Original image			
Shadow1			
Shadow2			
Sjadpw3			
Embedding of shadow2			
Embedding of shadow3			
Logo