# A Unified approach to construct Non-perfect Secret Sharing and Traitor Tracing schemes

**Kannan Karthik**
Electrical and Computer Engg.
University of Toronto
Toronto, Ontario, Canada

**Dimitrios Hatzinakos**
Electrical and Computer Engg.
University of Toronto
Toronto, Ontario, Canada

**Abstract** *In this paper, we explore some of the wonderful characteristics of the $C_{3,3} = [110; 101; 011]$ codebook when viewed from different angles. The information contained in this codebook implicitly carries the properties of inheritance, association and also a way to segment and mix two different binary sequences, thus, sowing the seed for taking a unified approach: (i) to construct simple non-perfect secret sharing schemes with traitor tracing properties, (ii) to facilitate simultaneous multiple information fusion and secure storage. (iii) to obtain different manifestations of a parent which can be used for authentication and tracing, (iv) to construct anti-collusion codes (ACCs), (v) to implement selective access schemes.*

*Keywords:* association, inheritance, traitor tracing, selective, MIX SPLIT

## 1 The $C_{3,3}$ codebook

There are several applications in which a single source of information (also called parent $I_{par}$) is used to create several descendants ($I_{child(i)}, i = 1, 2, ..n$). These children inherit several traits from their parent (which can be used to identify the original source). In addition, the information $I_{child(i)}$ is derived in such a way that unique associations are formed within different groups of siblings. The heart of this construction process is a simple binary codebook which controls the dissemination and composition of the children. To identify some potential applications, let us first study the beauty of this codebook,

$$C_{3,3} = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \quad (1)$$

Each row index corresponds to a child (or user) $i \in \{1, 2, ...n\}$ and the column index could be used to denote one of the following:

1. A mark or basis vector or a semi-fragile watermark $V_j, j = 1, 2, ..v$, which forms the basic building block of a digital fingerprint.
2. One of $v$ unique traits $V_j$ of $I_{par}$ which can be attributed to a particular child or group of children.
3. One of $v$ disjoint segments inherited from any one of two binary sequences $\bar{X}$ or $\bar{Y}$.

Each mark or trait can therefore be represented by a unique color and there are three different ways to interpret this information contained in the codebook.

### 1.1 Association

Firstly, it can be viewed as an association between the three codewords in $C_{3,3}$, $\bar{c}_1 = [110], \bar{c}_2 = [101], \bar{c}_3 = [011]$ (depicted as a colored graph in Fig. 1(a)). Each user is represented as a vertex in the graph and can be uniquely identified by the colors of the edges leaving a particular node $i$ (e.g. user $1 \equiv [V_1, V_2] \equiv \bar{c}_1$). On the other hand each user pair $(i, j)$ is represented by a different edge color (e.g. $(2, 3) \equiv [V_3] \equiv [0\ 0\ 1]$). The complete set (1,2,3) is represented by all three colors [$V_1$, $V_2$, $V_3$] $\equiv$ [1 1 1]. A reflection of the graph in Fig. 1(a) is the Table. 1, where one can see that a majority vote of any two or three codewords results in a unique bit pattern. This property has been used for constructing anti-collusion codes for tracking linear collusions in [1].

Table 1: Majority vote of subsets of codewords in $C_{3,3}$.

| Code | $\bar{c}_1$ | $\bar{c}_2$ | $\bar{c}_3$ | $\bar{c}_1, \bar{c}_2$ | $\bar{c}_2, \bar{c}_3$ | $\bar{c}_1, \bar{c}_3$ | $\bar{c}_1, \bar{c}_2, \bar{c}_3$ |
|---|---|---|---|---|---|---|---|
| MAJ | 110 | 101 | 011 | 100 | 001 | 010 | 111 |

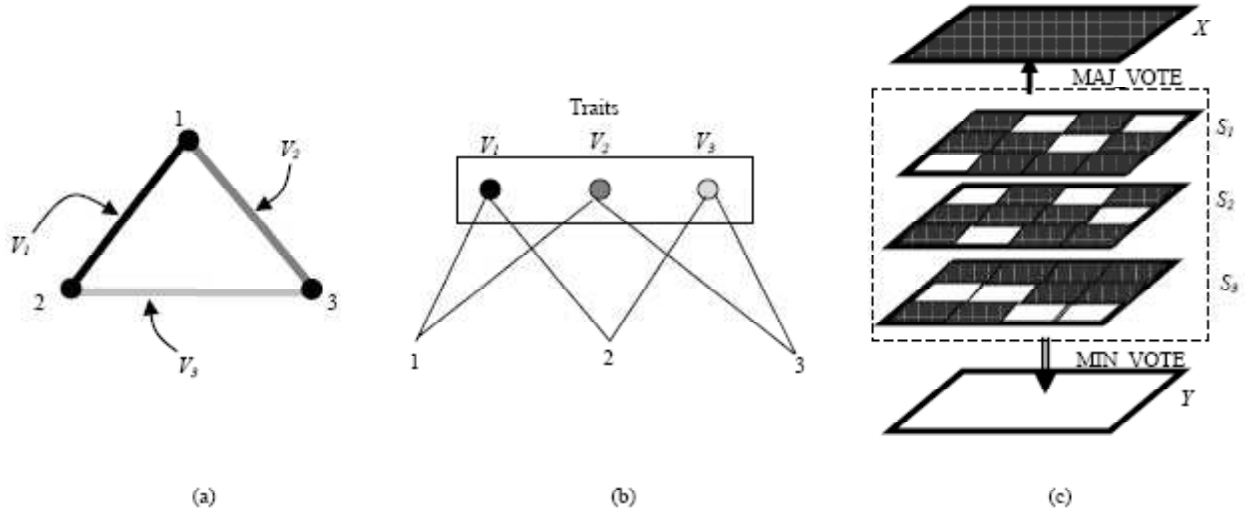


Figure 1: Three different ways to interpret the information contained in the $C_{3,3}$ codebook. (a) Association, (b) Inheritance, (c) Segmentation and mixing (MIX-SPLIT)

## 1.2 Inheritance

Fig. 1(b) shows another way to interpret the codebook in which the colors represent three unique traits of $I_{par}$. Each child $i$ inherits exactly two out of the three traits (e.g. Traits(child 1) = [$V_1$, $V_2$]). Even though the information acquired by the descendants is only a partial representation of the parent, it can be always be used to establish a link between $I_{par}$ and $I_{child(i)}$. One application of this property could be in the authentication of copies of a digital portrait. In this case, the concealed digital fingerprint not only captures some of features of the original portrait but also identifies the buyer.

## 1.3 Segmentation and mixing

In another view, the codewords $\{\overline{c}_1, \overline{c}_2, \overline{c}_3\} \in C_{3,3}$, can be thought of as three different shares created by first partitioning and then mixing *two* different secrets $\overline{X}$ and $\overline{Y}$, where, $\overline{X} = [x_1, x_2, ..x_L]$ and $\overline{Y} = [y_1, y_2, ..y_L]$ represent two sequences of independent and identically distributed (IID) binary random variables. Security of such a scheme is maximum if $x_i \perp x_j$ and $x_i \perp y_j$ for $i \neq j$, where $\perp$ denotes independence. This algorithm, called MIX-SPLIT is discussed in detail in [1] and presented in Algo. 1. It is the simplicity in the retrieval (Algo. 2) of secrets $\overline{X}, \overline{Y}$ from the shares $\overline{S}_1, \overline{S}_2$ and $\overline{S}_3$, which makes this scheme interesting and useful.

**input** : Codebook $C_{3,3}$, Sequences $\overline{X}, \overline{Y}$)
Permutation keys $K_{p1}, K_{p2}, K_{p3}$
**output**: Shares $\overline{S}_1, \overline{S}_2, \overline{S}_3$

Pos ← {1,2,..,L};
**for** $j \leftarrow 1$ **to** 3 **do**
  Pos ← Permute(Pos, $K_{pi}$);
  $P_j$ ← Pos(1:L/3);
  Pos ← SetDifference(Pos, $P_j$);
**end**
**for** $i \leftarrow 1$ **to** 3 **do**
  **for** $j \leftarrow 1$ **to** 3 **do**
    **if** $C_{3,3}(i,j) = 1$ **then**
      $\overline{S}_i(P_j) \leftarrow \overline{X}(P_j)$;
      **else if** $C_{3,3}(i,j) = 0$ **then**
        $\overline{S}_i(P_j) \leftarrow \overline{Y}(P_j)$ ;
      **endif**
    **endif**
  **end**
**end**

**Algorithm 1**: MIX-SPLIT (share generation)

**input** : Shares $\overline{S}_1, \overline{S}_2, \overline{S}_3$
**output**: Secrets $\overline{X}, \overline{Y}$

$\overline{X}$ ← MAJ_VOTE($\overline{S}_1$,$\overline{S}_2$,$\overline{S}_3$);
$\overline{Y}$ ← MIN_VOTE($\overline{S}_1$,$\overline{S}_2$,$\overline{S}_3$);

**Algorithm 2**: MIX-SPLIT (retrieval)

For retrieval, no key or codebook is required. $\overline{S}_1$, $\overline{S}_2$ and $\overline{S}_3$ can simply be stacked and then a majority bit vote can be evaluated to extract $\overline{X}$. The other secret $\overline{Y}$ is obtained through a minority vote. Several applications such as joint access with traitor tracing, secure multi-biometric storage etc can be conceived based on this algorithm [1].

**Cryptanalysis**

*Single share ($\overline{S}_i$):* Since the sequences, $\overline{X}$ and $\overline{Y}$ are statistically indistinguishable and the parti-

tions known only to the source, the probability that the attacker will succeed in affiliating a particular sub-sequence $\{\overline{S}_i(k_1), \overline{S}_i(k_2), .., \overline{S}_i(k_t)\}$, where, $\{k_1, k_2, ..k_t\} \subset \{1, 2, .., L\}$, to either $\overline{X}$ or $\overline{Y}$ is very small.

*Any two shares ($\overline{S}_i, \overline{S}_j$):* Let the length of each partition be $L_p = L/3$. Let the probability mass functions of $x_i$ and $y_i$ be $f_x = f_y = \{Pr(x = 0) = 0.5, Pr(x = 1) = 0.5\}$. In addition to this, $x_i \perp y_i$. The objective of the attackers is to create the best possible estimate of the secret $\overline{X}$ or $\overline{Y}$ using the two shares. The traitors will be aware of the structure of the codebook $C_{3,3}$, but oblivious to the hidden partitions $P_1, P_2, P_3$ and so can employ a bit comparison operation to identify the common portion ($P_{com(i,j)} = \{\text{all } k, \text{ s.t. } \overline{S}_i(k) = \overline{S}_j(k)\}$) to extract a small part of the sequence $\overline{X}$. Based on the probability mass function, the size of the set $P_{com(i,j)}$ is approximately $|P_{com(i,j)}| \approx L_p + 0.5L_p + 0.5L_p = 2L_p$. Hence, $|P_{diff(i,j)}| \approx L_p$. The question is from this set $P_{diff(i,j)}$ which positions correspond to $\overline{X}$ and which ones correspond to $\overline{Y}$. The attackers split this set into two equal disjoint sets $P_{diff(i,j)} = \hat{P}_{\overline{X}} \cup \hat{P}_{\overline{Y}}$. So the potential estimate of the secret is,

$$\widehat{X} = \overline{S}_i(P_{com(i,j)}) || \tilde{S}_A(\hat{P}_{\overline{X}}) || \tilde{S}_B(\hat{P}_{\overline{Y}}) \qquad (2)$$

where, '||' indicates the concatenation operator, $\tilde{S}_A(\hat{P}_{\overline{X}}) = \overline{S}_i(\hat{P}_{\overline{X}})$ and $\tilde{S}_B(\hat{P}_{\overline{Y}}) = BitComp[\overline{S}_i(\hat{P}_{\overline{Y}})]$. The function BitComp() represents a bit complement of the entire binary string. Now, the number of different types of partitions $\hat{P}_{\overline{X}}$ and $\hat{P}_{\overline{Y}}$ are $N_{part} = \binom{L_p}{0.5L_p}$. For $L = 300$ or $L_p = 100$, this number is $\binom{100}{50} \approx 10^{29}$. So this simple scheme is quite secure if the attacker(s) are allowed only a few attempts to reveal the secret $\overline{X}$ (as a part of a joint authentication process). Since, each share $\bar{S}_i$ is directly derived from $[\bar{X}, \bar{Y}]$, secret sharing is of non-perfect type (i.e. the conditional entropy $H(\bar{X}/\bar{S}_i) < H(\bar{X})$). In the following sections, we present two applications which use some or all the principles discussed above.

# 2 Authentication and tracing of copies of a digital portrait

In this application several perceptually similar copies $\{I_{c1}, I_{c2}, .., I_{cn}\}$ of an expensive digital portrait $I_{par}$ are created. From the point of view of the source, each copy must be traceable. This means by examining any copy one should be able to link it with the parent or creator, the buyer and in certain cases with traitors (involved in unauthorized resale of legitimate copies). This translates into the following security parameters:

*(a) Authentication* - This can be implemented by concealing a copyright watermark whose presence is an indication of the authenticity of the copy. This copyright watermark need not just carry information pertaining to its creator but also a blueprint of the digital portrait.

*(b) Fingerprinting* - This entails imprinting the buyer ID in the copy without altering its perceptual quality.

*(c) Integrity and Traitor tracing* - One primary reason for tampering is to conceal the identity of the buyer(s) which then opens up the possibility of redistribution. There could be several other motives. For example, the buyers could use the copy as a vehicle for conveying covert messages either by directly manipulating the artwork or by superimposing additional watermarks. There are two ways in which this tampering could be effected: (i) By careful localized image processing (single copy attack), (ii) By cleverly fusing several fingerprinted copies (multi-copy attack or collusion). Countermeasures demand a mechanism for not only localizing these manipulations but also for tracing these colluders. This can be implemented by embedding two sets of semi-fragile watermarks, each of which has very different characteristics:

1. Localized processing can be detected very effectively by concealing watermarks in the wavelet domain [2].

2. Traitor tracing or tracking collusion operations on the other hand require watermarks which are fragile to multi-copy fusion but robust to localized processing. One of the many [3], [4],[5] ways in which this can be achieved is by using a set of $v$ spatially orthogonal, DCT sign bit modulated marks as building blocks for constructing $n$ different fingerprints. The seed was sown in [6] and an anti-collusion code (ACC) tailored to track linear collusions (also effective against certain non-linear spatial domain fusion operations) is proposed in [1].

## 2.1 Architecture

Fig. 2 shows one way in which the above security parameters can be implemented. The blueprint $BP_1$ is a thin film of noise shaped by perceptual masking models, which is embedded in the wavelet domain as a semi-fragile watermark. Any manipulation of the copy, will disturb this film and this

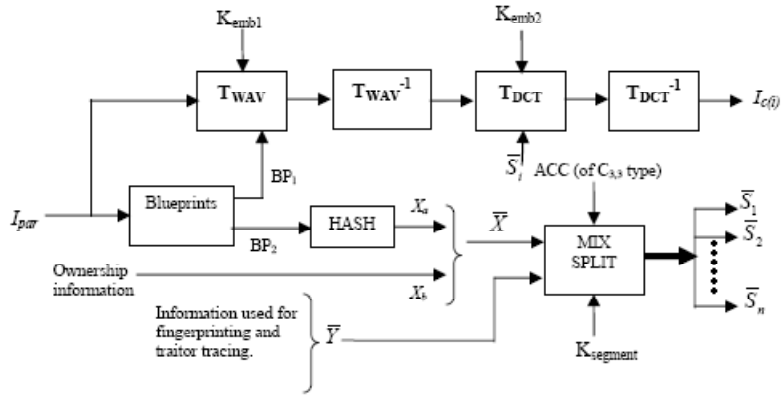


Figure 2: Security architecture for authenticating and tracking copies of digital portraits.

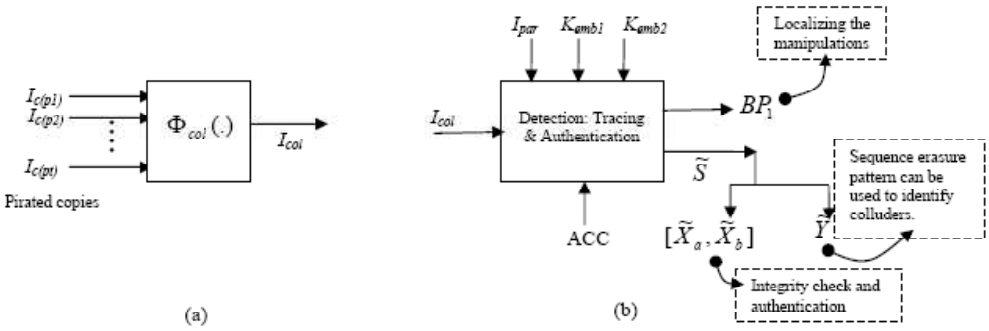


Figure 3: (a) Collusion model, (b) Parameters involved in authenticating retrieved copies.

disturbance can be localized thanks to the space-frequency localization characteristics of the wavelet transform [2]. $BP_2$ is the sign plane of perceptually relevant AC coefficients (after computing a block discrete cosine transform). Since this entire plane cannot be concealed, a hash of it $\bar{X}_a = Hash(BP_2)$ is calculated. This information is combined with some proof of ownership $\bar{X}_b$ to form the binary sequence $\bar{X}$. This is mixed with another random sequence $\bar{Y}$ using the MIX-SPLIT algorithm. The erasure of the information contained in $\bar{X}$ confirms that some tampering has been done and the erasure pattern of $\bar{Y}$ can be used to detect collusion operations and identify some or all the traitors (aided by the association property of the codebook in Section. 1.1). Since each share $\bar{S}_i, i = 1, 2, ..n$ has a unique signature (compiled by mixing different segments from both $\bar{X}$ and $\bar{Y}$), it also serves as a fingerprint for identifying the buyer. Only a subset of the segments in $\bar{X}$ are inherited by each copy which can be used to establish legitimacy and also link it to the parent. A model of the multi-copy collusion operation is given in Fig. 3(a) and the parameters used for tracing and authentication in Fig. 3(b).

Examples of ACC books which can be used are,

**(i)** All Hadamard 2-designs (with $v = n = 4k - 1, k = 1, 2, 3, ..$). Example is $C_{3,3}$ (Eqn. 1).

**(ii)** Codebooks used for $(n, n)$ joint access problem [1]. $C_{3,3}$ is also a member of this family.

# 3 Selective access

There are several intelligence applications in which *different segments* from a covert surveillance video, a top secret document, a geographical map or even a strategic plan conveys information of varying importance, accessible to only a very small select group of users. Fig. 4(a) shows one access scenario, in which three groups have access to different portions of an encrypted map. Users {1,2,3} can jointly see the contents in window $W_1$, users {1,5} window $W_2$ and {4,6} $W_3$. This can be implemented using a secret sharing scheme. We apply some of the properties of the $C_{3,3}$ codebook (Sections. 1.2, 1.3) to a simpler example in Fig. 4(b).

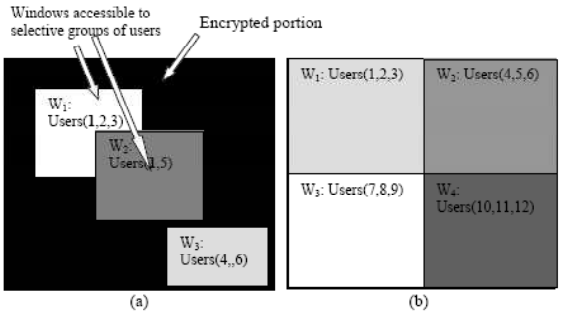


Figure 4: (a) A general access scenario, (b) Example implemented.

### 3.1 Algorithm description

Based on the example in Fig. 4(b), a map $I_m$ has four windows $W_1, W_2, W_3, W_4$ of equal size. The joint access assignment is as follows: $\{1,2,3\} \mapsto W_1$, $\{4,5,6\} \mapsto W_2$, $\{7,8,9\} \mapsto W_3$ and $\{10,11,12\} \mapsto W_4$. The implementation requires $v = 12$ carefully designed shares $\bar{S}_1, \bar{S}_2, .., \bar{S}_{12}$. One important requirement is that of containment i.e.,

$$\text{Info}(\bar{S}_1) \subset \text{Info}(\bar{S}_1, \bar{S}_2) \subset \text{Info}(\bar{S}_1, \bar{S}_2, \bar{S}_3) = W_1 \quad (3)$$

Similar requirements for the other three windows. From a more practical point of view, the decryption key shares must be designed in such a way that $\text{Info}(\bar{S}_1, \bar{S}_2)$ or $\text{Info}(\bar{S}_1)$ will result in a highly distorted window $W_1$,

$$\begin{aligned} \text{Decrypt}[I_{Em}, \text{Info}(\bar{S}_1, \bar{S}_2)] &<< \delta_p(W_1) \\ \text{Decrypt}[I_{Em}, \text{Info}(\bar{S}_1, \bar{S}_2, \bar{S}_3)] &> \delta_p(W_1) \end{aligned} \quad (4)$$

where, $I_{Em}$ represents the encrypted version of map $I_m$ and $\delta_p(W_1)$ the perceptual similarity threshold for viewing the contents of window $W_1$ clearly. As in the case of the MIX-SPLIT (Section. 1.3), each of the shares $\bar{S}_i$ are constructed from two binary sequences $\bar{X}$ and $\bar{Y}$, where the latter represents the encryption key. The codebook which has the property Eqn. 3 and controls the composition of the shares is,

$$C_{12,3} = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}$$

Just as in the MIX-SPLIT, a share $\bar{S}_i, i = 1, 2, ..12$ is given by,

$$\bar{S}_i = \bar{S}_i(P_1)||\bar{S}_i(P_2)||...||\bar{S}_i(P_{12}) \quad (5)$$

where for $j = 1, 2, 3, .., 12$ and random partitions $P_1$, $P_2$,.., $P_{12}$,

$$\bar{S}_i(P_j) = \bar{Y}(P_j) \text{ if } C_{12,3}(i,j) = 0 \quad (6)$$

$$\bar{S}_i(P_j) = \bar{X}(P_j) \text{ if } C_{12,3}(i,j) = 1 \quad (7)$$

The information to be encrypted is chosen as the sign plane of the most significant discrete cosine transform (DCT) AC coefficients denoted by the $L$-bit binary vector $\bar{Z}_{SP}$. Encryption of $\bar{Z}_{SP}$ ensures complete obscurity of the map $I_m$. The encryption process is simply,

$$\bar{E}_{SP} = \bar{Z}_{SP} \oplus \bar{Y} \quad (8)$$

For the four groups of users $k = 1, 2, 3, 4$, the keys for joint decryption can be obtained by stacking three $L$-bit shares $\bar{S}_q$, $\bar{S}_{q+1}$, $\bar{S}_{q+2}$ and evaluating a minority bit vote,

$$\bar{D}_{SP(k)} = \text{MIN\_VOTE}(\bar{S}_q, \bar{S}_{q+1}, \bar{S}_{q+2}) \quad (9)$$

where, $q = 3(k-1)+1$. Note that, although the codebook is labeled as $C_{12,3}$, only four out of $\binom{12}{3} = 220$, are legitimate triplets, which will meet both Eqns. 3 and 4. Only those minority vote outputs, which contain the right combination of buried subsequences $[\bar{Y}(P_e), \bar{Y}(P_f), \bar{Y}(P_g)]$, $e, f, g \in \{1, 2, .., 12\}$, will serve as a group decryption key $\bar{D}_{SP(k)}, k = 1, 2, 3, 4$.

### 3.2 Simulation

The test image used is a map of some town (256×256 gray scale PGM image). The size of significant sign plane is 1024×50, which implies the first fifty DCT-AC coefficients from all the 1024, $8 \times 8$ blocks are chosen for encryption. The size of the all the shares is 6.25KB. The original and the encrypted map are shown in figures. 6(a) and (b) respectively. A legitimate joint access of three users from groups 1,2,3 or 4 results in Figs. 6(c,d,e,f) where one can see that only the contents in the window $W_i$ are visible (the rest of the map is deliberately left distorted). Fig. 6(g) is an example of an illegitimate access in which two users {1,3} try to view the contents of $W_1$ by finding different ways to fuse the information in the shares $\bar{S}_1$ and $\bar{S}_3$. There are several ways in which this share fusion attack can be implemented, one of which is based on iterated share mixing (illustrated in Fig. 5). The 'MIX'

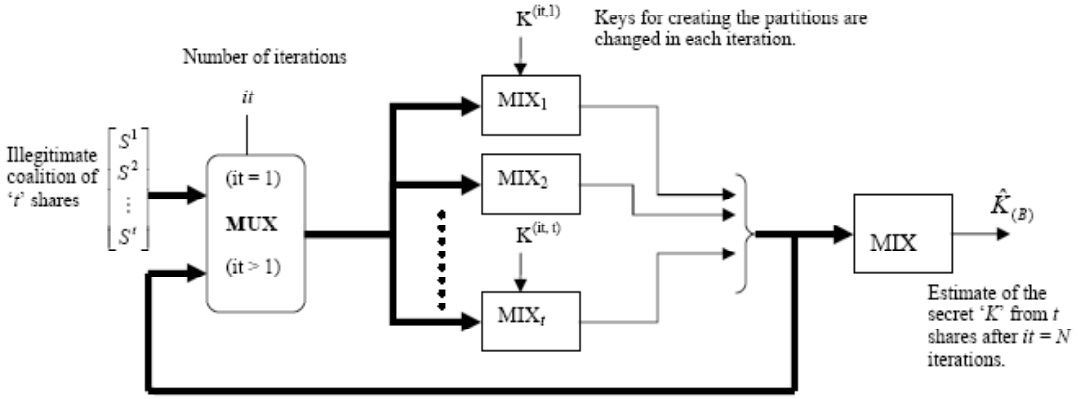


Figure 5: Iterated share mixing attack.

stage used in this algorithm is discussed in Algo. 3.

**input** : (1) Shares with $t$ traitors, $\{S^{(1)}, S^{(2)}, .., S^{(t)}\}$.
(2) Permutation keys $K_{p0}, K_{p1}, ..K_{pt}$.
**output**: Resultant share after the mixing operation.

$P = [1, 2, 3, ...L]$; *'L' bit positions within the share*
$L_t \leftarrow$ `Floor`$(L/t)$;
$R \leftarrow$ `Permute`$(P, K_{p0})$;
**for** $j \leftarrow 1$ **to** $t$ **do**
  $Q_j \leftarrow R(1 : L_t)$;
  $R \leftarrow$ `SetDifference`$(R, Q_j)$;
  $R \leftarrow$ `Permute`$(R, K_{pj})$;
**end**
$\hat{K}_B \leftarrow$ `Union`$(S^{(1)}[Q_1], S^{(2)}[Q_2], ..., S^{(t)}[Q_t])$

**Algorithm 3**: 'MIX' stage in share mixing attack shown in Fig. 5.

The number of iterations specified in this attack was 200. Results show that despite using this share mixing attack, map details in window $W_1$ are protected. Fig. 6(h) shows an example of an illegal collusion across groups in which users {1,3} from group 1 attempt to combine the information with users {7,8} (group 3) to view the contents of windows $W_1$ and $W_3$. This fusion is also unsuccessful as contents of neither window are visible (Fig. 6(h)).

# 4 Conclusions

The information contained in $C_{3,3}$ codebook carries the properties of inheritance, association and also a way to mix and split two different binary sequences. Traces of these properties are visible in both the applications discussed in this paper. The paper thus, sows the seed for taking a unified approach: (i) to construct simple non-perfect secret sharing schemes with traitor tracing properties, (ii) to facilitate simultaneous multiple information fusion and secure storage. (iii) to obtain different manifestations of a *parent* which can be used for authentication and tracing, (iv) to construct anti-collusion codes (ACCs), (v) to implement selective access schemes.

# References

[1] K. Karthik, "Methodologies for access control and fingerprinting of multimedia," in *Ph.D. Thesis, University of Toronto*, 2006.

[2] D. Kundur and D. Hatzinakos, "Towards a Telltale Watermarking Technique for Tamper-proofing," in *Proc. ICIP*, vol. 2, (Chicago, Illinois), pp. 409–413, Oct 1998.

[3] J. Dittmann, A. Behr, M. Stabenau, P. Schmitt, J. Schwenk, and J. Uederberg, "Combining digital watermarks and collusion secure fingerprints for digital images," in *SPIE Intl. Conf. on Electronic Imaging*, vol. 41, pp. 171–182, 1999.

[4] D. Boneh and J. Shaw, "Collusion secure fingerprinting for digital data," *IEEE Transactions on Information Theory*, vol. 44, pp. 1897–1905, Sept 1998.

[5] W. Trappe, M. Wu, J. Zang, and K. J. R. Liu, "Anti-collusion Fingerprinting for Multimedia," *IEEE Transactions on Signal Processing*, vol. 51, pp. 1069–1087, April 2003.

[6] K. Karthik and D. Hatzinakos, "Decryption Key Design for Joint Fingerprinting and Decryption in the Sign Bit Plane for Multicast content protection," *International journal of Network Security (accepted Nov 17, 2005)*, vol. 4, pp. 254–265, May to be published in May 2007, http://ijns.nchu.edu.tw/contents/ijns-v4-n3/ijns-2007-v4-n3-p254-265.pdf.

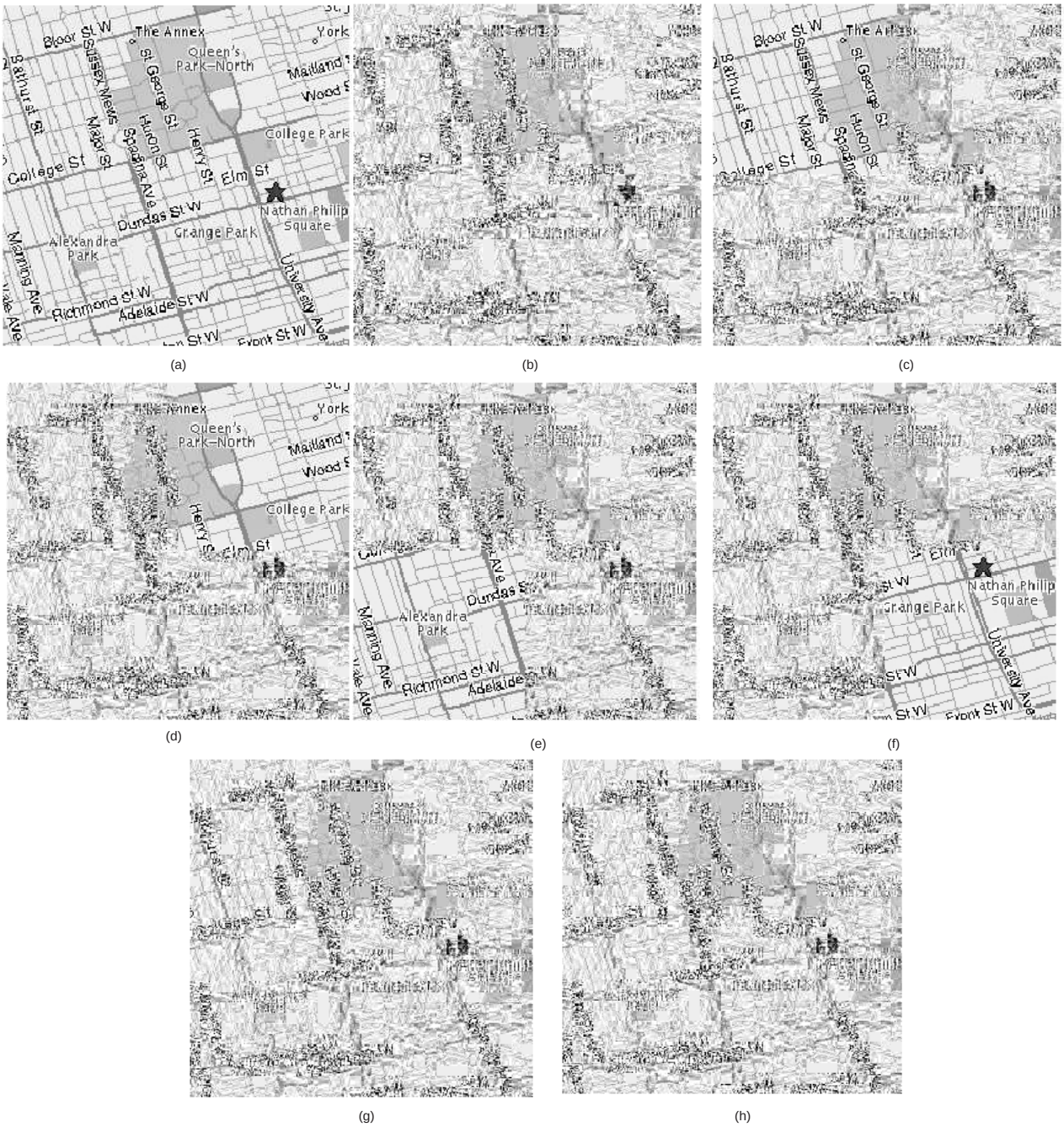


Figure 6: (a) Original, (b) Encrypted, (c) Decrypted by group-1 $\bar{S}_1, \bar{S}_2, \bar{S}_3$, (d) Decrypted by group-2 $\bar{S}_4, \bar{S}_5, \bar{S}_6$, (e) Decrypted by group-3 $\bar{S}_7, \bar{S}_8, \bar{S}_9$, (f) Decrypted by group-4 $\bar{S}_{10}, \bar{S}_{11}, \bar{S}_{12}$, (g) Illegitimate fusion using attack shown in Fig. 5 by users 1,3 $[\bar{S}_1, \bar{S}_3]$, (h) Illegitimate fusion across groups i.e. users 1,3,7,8