Chapter 26
Threshold Secret Sharing Scheme for Compartmented Access Structures

P. Mohamed Fathimal
Manonmaniam Sundaranar University, India

P. Arockia Jansi Rani
Manonmaniam Sundaranar University, India

ABSTRACT

In the realm of visual cryptography, secret sharing is the predominant method of transmission and reception of secure data. Most of the (n, n) secret sharing schemes suffer from one common flaw — locking of information when the all- n number of receivers are not available for some reason. This paper proposes a new method of compartmented secret sharing scheme where some threshold number of equally privileged from each compartment can retrieve data. This scheme rules out regeneration of secret image at the single compartment thereby eliminating the danger of misusing secret image. The key features of this scheme are: better visual quality of the recovered image with no pixel expansion; non-requirement of half toning of color images; less computational complexity by reconstructing secret through XORing and simple addition of all share images. This scheme is highly beneficial in applications where data has to be stored securely in a database and in cloud computing to synchronize information passed to different groups or clusters from a single host.

INTRODUCTION

In today's information and networking era, secret sharing is a fundamental issue in network security. Many applications such as distributed file storage, key management and multi-party secure computation use secret sharing scheme to share a secret among a set of participants. Shamir (1979) and Blakley (1979) introduced this secret sharing scheme in 1979. In this threshold (t, n) secret sharing scheme, secret

DOI: 10.4018/978-1-7998-1763-5.ch026

shares are distributed to n participants and the secret image is reconstructed by combining more than t of them. In this scheme, all participants have equal privileges and cannot be distinguished according to trust or authority and only the number of the participants involved is important for recovering the secret.

Multi-level secret sharing scheme is a scheme in which each participant is assigned a level — a positive integer — and at least r participants of each level are required to access the secret. There are two categories of multi-level access structure. The first category is the hierarchical structure in which the participants differ in their authority or level of confidence and the presence of higher-level participants are authoritative to allow the recovery of the secret. The electronic fund transfer in a bank may require the signature of two vice-presidents or three senior tellers for authentication. If there are only two senior tellers available, then the third senior teller role can be played by a vice-president.

The second category of multi-level secret sharing scheme is multipartite or compartmented secret sharing scheme in which every compartment or part has some number of equally privileged participants. The reconstruction of the secret requires a specified level of concurrence by participants in all the compartments. When two companies agree to sign the secret document through a secret sharing scheme, regeneration of the secret document is possible only when at least threshold number of the participants from both companies pool their shares together.

This paper proposes an ideal compartmented secret sharing scheme using magic square for situations requiring the agreement of several parties to recover the color secret image.

RELATED LITERATURE REVIEW

Many researchers introduced new secret sharing scheme based either on Shamir's scheme (1979) or with new concepts. Shamir introduced multipartite access structures in his seminal work for weighted threshold access structures. Blakely (1979) introduced geometric threshold secret sharing scheme. Mignotte (1983) and Asmuth-Bloom (1983) developed threshold secret sharing scheme based on the Chinese remainder theorem.

Mignotte's threshold secret sharing scheme (1983) uses special sequences of integers, referred to as Mignotte sequences. A (k, n)-Mignotte sequence is a sequence of positive integers $m_1 < \cdots < m_n$ such that $(m_{i,}\ m_j) = 1$, for all $1 \leq i < j \leq n$, and $m_n - k + 2 \cdots m_n < m_1 \cdots m_k$. The scheme proposed by Asmuth and Bloom (1983) also used special sequences of integers. More exactly, a sequence of pairwise coprime positive integers r, $m_1 < \cdots < m_n$ is chosen such that $r \cdot m_n - k + 2 \cdots m_n < m_1 \cdots m_k$. This scheme was generalized for allowing modules that are not necessarily pairwise coprime in an obvious manner.

Brickell (1990) proposed an elegant solution by choosing the secret S as a combination of m compartment secrets and using a threshold secret sharing scheme for each compartment. In the reconstruction phase, if the number of participants from the j^{th} compartment is greater than or equal to the k_j, for all $1 \leq j \leq m$, then all compartment secrets can be recovered and thus the secret S can be obtained. Brickell proved that all multilevel and compartmented access structures are ideal. He proved that every structure in one of those families admits a vector space secret sharing scheme over every large enough field. Even though the proof is constructive, this scheme did not explain how to construct efficiently.

Simmons (1990) introduced two families of multipartite access structures, the so-called multilevel and compartmented access structures by generalizing the geometrical threshold scheme by Blakely (1979) and he speculated that this was possible for all of them. He has presented the example of an official action that requires at least two Americans and at least two Russians for its initiation.