Abstract

In today's scenario many audio/voice files are needed to be transmitted over internet for various important purposes. So protection of these files is an important issue. Efficient cryptographic methods are there to protect data but every thing depends on the protection of encryption key. That leads to single point failure. To overcome this drawback shared
cryptography becomes more popular. Here we are suggesting a novel secret sharing scheme which employs simple graphical masking method, performed by simple ANDing for share generation and reconstruction can be done by performing simple ORing the qualified set of legitimate shares. Not only that, the generated shares are compressed and each share contains partial secret information, that leads to added protection to the secret and reduced bandwidth requirement for transmission.

Reference

- Bozkurt, Kaya, Selcuk, Guloglu “Threshold Cryptography Based on Blakely Secret Sharing” Information Sciences.

Index Terms

Computer Science       Security
Key words

- Threshold Cryptography
- Audio sharing
- Compression
- Perfect Secret Sharing (PSS)