Introduction

Cryptography is a process of changing the human readable message into the human unreadable message. In computer science the cryptography is used to secure the system such as encrypting passwords, messages etc. One of the cryptographic techniques which allow visual information to be encrypted is visual secret sharing. Other than plain text it is used to encrypt the images and pictures. In Visual cryptography the secret image is encoded into multiple shares. It was first purposed by Moni Naor and Adi Shamir in 1994 in Eurocrypt. Here image 'I' is divided into 'n' shares. 'I' can be constructed from 'k' shares out of 'n'. Complete knowledge of 'k-1' share cannot decrypt the 'I'. So, this type of cryptographic scheme remains more secure. Visual secret sharing uses threshold scheme by using the concept of Lagrange's polynomial interpolation. Applying XOR operation with cover image leads to authentication of secret. The reconstruction of the original image without loss of information can be generated form shared shares using the concept of Lagrange's polynomial interpolation. Visual secret sharing schemes are used to manage image data protection as well as image based authentication techniques that contain sensitive data such as military surveillance, satellite images, medical records, financial transactions, electronic voting systems, maps, encrypted data etc. In this study visual secret share scheme are going to implement and analyze with different parameter like NPCR, UACI, correlation-coefficient, performance speed measures.

Problem Definition

Visual cryptography provides secure means to transfer crucial data on the Internet. To manage the security issues of very confidential data. If offers efficient solutions for controlling private data and images that are made available only to selected people.

In traditional image steganography the image is simply encoded and distributed to participants, such that human eye can recover the secret image by overlapping the minimum required transparencies shares without any mathematical computation. In few traditional cryptography the encryption and decryption process need high computation costs and need secret key for decoding. The visual secret sharing scheme help to maintain data confidentiality while transferring file over insecured network such as internet. Visual cryptography schemes allow the encoding of a secret image into shares, which are distributed on the participants. The condition for minimum threshold share requirement ultimately leads to the confidentiality of secret. Shamir's (k, n) visual secret sharing uses threshold scheme by using the concept of Lagrange's polynomial interpolation. The reconstruction of the original image without loss of information can be generated from shared shares without complex mathematical calculation. So visual cryptography has less computation cost and does not require secret key. In addition it is easy and fast to decode.

Scope and objective

scope

Cryptography is used to strength the security of system mostly in computer based systems. The visual secret sharing can be used in biometric security, watermarking, steganography, bank customer identification etc.

Objectives

The mean objective of the project is:

* To know the function of secret sharing scheme to distribute the shares among multiple parties and reconstruct the secret that has been shared as shares among parties with at least minimum required threshold shares/parties bring together.
* To implement the visual secret sharing scheme by using Shamir's and Proactive secret sharing scheme performance of both scheme on visual secret.
* To analyze the performance, pixels change rate, unified average change Intensity and correlation coefficient of the generated shares with the secret variation of shares threshold number

Research methodology

Visual cryptography is a new type of cryptographic scheme that focuses on solving the problem of secret sharing. Visual cryptography is a desirable scheme as it embodies both the idea of perfect secrecy and a very simple mechanism for decrypting/ decoding the secret without complex computation.

The methodology includes implementing the Shamir's and Proactive Secret Sharing scheme algorithms applied in pixel value of secret image after embedding (XORed) with cover images. The secret and cover images are standard images. The details of data collection are discussed in section 4.3. The reason for using Shamir secret share scheme is to generate shares from the secret so that when applied minimum threshold shares reveal the secret. Proactive secret shares will generate updates shares periodically to prevent from intruder's access to the secret. Each pixel from original image works as secret. To share this secret among n participants first extract A, R, G and B component of image pixels. Then apply Shamir (k, n) visual secret sharing where each individual components becomes secret to share.

The Shamir's secret sharing and Proactive Secret sharing are used to share secrets among parties. Both the Shamir's and Proactive secret sharing scheme uses threshold scheme. These scheme deals with the confidentiality of the secret but not the authentication of secret that has been shared. To make the shared secret confidential as well as authentic, Secret image's pixel is embedding (XOR) with Cover image's pixels bitwise and apply Shamir and Proactive scheme on generated result of XORed operation to share this secret information as shares. The visual secret will be reveal only when minimum number of shares are available defined while constructing the shares for the reconstruction and apply bitwise XOR operation with cover image's pixels to reveal the secret/key image. The only condition is that both the sender and receiver should have same cover image.

Algorithms:

The Shamir's secret sharing and Proactive Secret sharing are used to share secrets among parties. Both the Shamir's and Proactive secret sharing scheme uses threshold scheme. These scheme deals with the confidentiality of the secret but not the authentication of secret that has been shared. To make the shared secret confidential as well as authentic, Secret image's pixel is embedding (XOR) with Cover image's pixels bitwise and apply Shamir and Proactive scheme on generated result of XORed operation to share this secret information as shares. The visual secret will be reveal only when minimum number of shares are available defined while constructing the shares for the reconstruction and apply bitwise XOR operation with cover image's pixels to reveal the secret/key image. The only condition is that both the sender and receiver should have same cover image.

**3.2.1 Shamir (k, n) Threshold Scheme Share Generation and Reconstruction**

Secret sharing using allows each party to keep a portion of the secret and provides a way to know at least part of the secret. Encryption using multiple keys is a possible solution for secret sharing. However, this solution requires a large number of keys, therefore the management of such a scheme becomes troublesome, as demonstrated by Shamir.

A secret sharing scheme enables distribution of a secret amongst n parties, such that only predefined authorized sets will be able to reconstruct the secret. Threshold schemes are ideally suited to applications in which a group of mutually suspicious individuals with conflicting interests must cooperate. By properly choosing the k and n parameters we can give any sufficiently large majority the authority to take some action while giving any sufficiently large minority the power to block it [16].

Lagrange interpolation is used to reveal the secret from generated shares with minimum number of required shares. It is the problem of constructing function which goes through a given set of data points [22]. Lagrange gave the following interpolation polynomial q(x) of degree n given at (n+1) points (xi, yi) i=0,1,…,n. such that :

y = q (x) = ∑ 𝑦𝑖 𝑙𝑖 𝑛 𝑖=0 (𝑥) ………………………………………………..Eq(1).

where, yi is shared value same as Di defined by Adi shamir [12,16].

Where li(x) is Lagrange basic polynomial defined by

li(x) = ∏ (𝑥−𝑥𝑖) (𝑥𝑖 −𝑥𝑗) 𝑛 𝑗=0 𝑖≠𝑗 ……………………………………………………..Eq(2).

11

**Share Generation:**

Step 1: Take inputs n as total shares and k as minimum number of require threshold to recover secret.

Step 2: Generate polynomial equation of degree (k-1) as q(x)=ao+alx+ . . . +ak-1xk-1 mod p, where ao=pixel value and ao, a1, ….,ak-1<p, p is large prime.

**Secret Reconstruction:**

Step 1: apply Lagrange interpolation with minimum required threshold shares as:

y = q (x) = ∑ 𝑦𝑖 𝑙𝑖 𝑛 𝑖=0 (𝑥) mod p …………………………………………..Eq(3).