HyperSpectral Image Secret Sharing using Shamir Scheme

Modigari Narendra, L. Jani Anbarasi, P. Kanmani, A. Mohanadevi
Department of CSE
Sri Ramakrishna Institute of technology
Pachapalyam, Coimbatore-641010
e-mail: narendramodigari@gmail.com
Janiherbert79@gmail.com
mailme.kanmani@gmail.com

Department of CSE
Jerusalem College of Engineering
Pallikkaranai, Chennai-600100
mohanadevi_237@yahoo.in

Abstract

Secret sharing refers to a process of distributing a secret among a group of participants, where each participant is issued with a share of the secret. The secret can be reconstructed by combining the participants’ shares. Single individual participants share is of no use. This paper proposes a (t, p) secret sharing approach for hyper spectral images using Shamir model. The secret hyper spectral image pixels and the participant’s numerical key are used in the reversible polynomial function to generate ‘p’ secret shares. The dealer distributes the generated secret shares to ‘P’ participants’ . During reconstruction the Lagranges interpolation process is used to reconstruct the secret hyper spectral image. The secret is reconstructed by combining atleast ‘t’ secret shares. The secret is reconstructed without loss.

1. Introduction

All Security is an important issue in information technology which rules the internet world today. The main issues in security are confidentiality, security, and authentication. Visual cryptography and visual secret sharing are used to securely share a secret among a various participants. Sensitive and important data are generally shared secretly using visual secret sharing method. The secrets are encrypted into P shares and are distributed to various participants. The participant’s shares are pooled together to reconstruct the secret. In (t, p) scheme the secret is divided in to p shares where t shares are needed to reconstruct the original secret. No information’s can be retrieved from Single participant share.

Blakley and Shamir[1] proposed (t, p) threshold scheme, in the year 1979 where a dealer securely shares and divides the secret into n number of shares. The dealer distributes these shares to the authorized participants where atleast t, authorized participants reconstruct the secret data using their corresponding shares by cooperating among themself..

Shamir [1] proposed Visual secret sharing where the Secret is encoded into random images called shares where the shares are transmitted instead of secret. This method suffers pixel expansion, image loss, and meaningless. Since meaningless shares are attracted towards intruders Wang [5] and Chen et al [8] proposed an approach where steganographic technique is used to hide the shares in to another host image called stego images. The meaningful shares avoid the suspicion of intruders.

Lin and Tsai [10] and Wu, Y.S., Thien, C .C., Lin [11] proposed a (t,p) secret sharing scheme that generates shadows based on t-1 polynomial. These shadows are embedded into a host image to generated stego images. In this method the secret pixel values greater than 250 are truncated to 250 which leads to loss of secret which is not tolerable for medical and important data’s.

These drawbacks are avoided by Thien and Lin [12], Chang et al. [9] and Zhao et al. [13] by representing gray values larger than 250 as two pixel values . Secret color image was securely shared along with steganographic technique where both secret and the host image was retrieved successfully in [15]. In [16] multiple gray images was securely shared using YCH scheme along with verifiability property.

Visual Cryptography proposed by Naor and Shamir [13] encodes a binary secret into two shares based on white and black pixels and the secret is reconstructed by superimposing the two shares. Two binary secrets are securely shared using Halftoning in [17,18].
Hyper spectral image secret sharing is proposed using Shamir secret sharing in our paper which possesses reversible characteristics as [13]. Hyper spectral images are securely shared among participants where at least t participants pool their shares to reconstruct the secret. During reconstruction the secret is retrieved without any distortion.

The rest of the article is organized as follows. Section II explains about Shamir’s threshold scheme. Section III explains the various modules of proposed work. Experimental simulation results and performance analysis are explained in section IV. Conclusion and Future enhancement is discussed.

2. Related work

Related work includes Shamir’s secret sharing approach. In this approach, a secret S and a prime number m are used to generate a (t-1) degree polynomial.

\[ F(X) = S + C_1X^1 + \ldots + C_{t-1}X^{t-1} \mod m \quad (1) \]

Where \( S \) is the secret value and the other coefficients \( C_1, C_2, \ldots, C_{t-1} \), are random numbers between 0 to m-1.

\[ Y_i = F(K_i) \quad Y_2 = F(K_2) \quad \ldots \quad Y_p = F(K_p) \quad (2) \]

Where \( Y_i \) (1 ≤ i ≤ p) are the computed share value and are issued to ‘P’ participants by the dealer. During reconstruction at least t shares are pooled by the participants and the secrets are reconstructed using Lagrange’s interpolation polynomial. The reconstruction of the secret is given in (3)

\[ F(x) = \sum_{i=1}^{t} \sum_{j=1}^{t} \prod_{i \neq j} \frac{x - k_j}{k_i - k_j} \mod m \quad (3) \]

3. Proposed Work

Overview of this paper is explained in this paper. Secret sharing is obtained in two modules. Share creation and Secret reconstruction. Band separation and generation of shares are the two phases in the first module followed by Secret reconstruction in the second module using Lagrange’s interpolation technique.

3.1 Share Creation

3.1.1 Band Representation:

Hyper spectral images are securely shared using Shamir secret sharing. Hyper spectral image comprises of multiple number of bands. Each band is separated band is represented as \( S_i \) (1 ≤ i ≤ n). Number of bands chosen for secret sharing should be less than the threshold.

3.1.2 Shadow Derivation:

Secret sharing is a process of dividing a secret image into n number of shadow images. The secret hyper spectral image pixels are used as the coefficient of the polynomial and using prime number m the values of the shadows are reduced between 0 to m-1 modulo operation. Let \( S_1, S_2, \ldots, S_n \) are the pixels of the secret bands. This secret pixels are used as the polynomial function \( F(x) \) where number of bands ‘n’ should be less than the threshold ‘t’. Substituting the pixels in (1) \( F(X) \) can be generated as

\[ F(X) = S_1 + S_2X^1 + \ldots + S_nX^{n-1} \mod m \quad (4) \]

Secret Key value \( K_i \) where (1 ≤ i ≤ p) of each participant are substituted and the shadow value \( Y_i \) (1 ≤ i ≤ p) are calculated and are distributed to P participants.

3.2 Secret Reconstruction

Secrets can be reconstructed only when at least t shares are pooled together, less than t shares is of no use. The secret can be computed using the Lagrange’s formula participant’s key and shadow value.

The Lagrange’s interpolation formula is given below

\[ F(x) = \sum_{i=1}^{t} Y_i l_i(x) \mod m \quad (5) \]

In this \( F(x) \) is Lagrange’s interpolation where, \( Y_i \) is shadow value and \( l_i \) is calculated using participant’s numerical key \( K_i \).

\[ l_i(x) = \prod_{i=1; i \neq j}^{t} \frac{x - k_j}{k_i - k_j} \mod m \quad (6) \]

The polynomial \( F(x) \) is reconstructed from which every secret pixels are grouped together to form the secret bands of the hyper spectral image. The secret is reconstructed without loss.
4. Simulation Results

The performance and the simulation of the proposed scheme are analyzed and explained in this section. The experimental platform was programmed in Matlab version 7.9. The secret hyper spectral image and the separated three bands are shown in Figure 2.

During reconstruction at least three shares are pooled to reconstruct the secret. The dealer reconstructs the secret using the secret key of the participant and the pooled secret. The reconstructed secret bands are shown in Figure 4 and finally the hyperspectral band is reconstructed.

6. Conclusion

The proposed reversible image sharing approach for hyper spectral image shows that secret hyperspectral image is securely shared and is reconstructed without loss. The generated shadows are meaningless. Based on (t, p) threshold scheme, any t authorized recipients can recover the secret by using the reversible process. This methodology can be further enhanced for the generation of meaningful shares.
References


