ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 6, June 2013

PROTECTED COLOR IMAGE TRANSMISSION USING STEGANOGRAPHY BASED ON SHAMIR'S THRESHOLD

Ashwini.kuradagi[1], Prof. Sarojini. B .K[2]

M.Tech, Digital Communication, Basaveshwar College of Engineering , Bagalkot, Karnataka,India[1]

Dept of E&C, Bagalkot, Karnataka, India[2]

Abstract: Steganography has become one of the most fascinating research areas in recent years. Steganography is a kind of data hiding technique that provides another way of security protection for digital image data. It is usually applied in various digital media types such as image, video, and audio at present. We present a new image sharing method based on Shamir's (t, n) threshold scheme. In this paper we are considering two color images , one as cover image and other as secret image. Secret image is hidden in cover image. Quantization process is applied to improve the quality of the cover image .In (t, n) threshold scheme, where a dealer encrypts and divide the secret into n number of shadows. The dealer then distributes the shadows to the authorized participants. Any t out of n, authorized participants can cooperate to reveal the secret data with their corresponding shadows. Single individual participants share is of no use. Peak signal to noise ratio is applied to analyze the quality of the stego images. The simulation results show that the secret and cover are reconstructed without loss.

Keywords: Secret image sharing; Steganography,Stego-image, (t, n)-Threshold Scheme.

I. INTRODUCTION

Due to fast growth of Internet applications, digitized data becomes more and more popular. Because of the ease of digital duplication and tampering, data security becomes an important issue nowadays. In certain application cases, it is a risk if a set of secret data is held by only one person without extra copies because the secret data set may be lost incidentally or modified intentionally.So it might be necessary for a group of persons to share a certain set of secret data.Shamir proposed first the concept of (t, n) threshold secret sharing to solve this problem. The scheme is designed to encode a secret data set into n shares and distribute them to n participants, where any t or more of the shares can be collected to recover the secret data, but any t-1 or fewer of them will gain no information about.

II Review of Related Works

The proposed approach to secret image sharing is based on the (t, n) threshold secret sharing method proposed by Shamir[1]. In Shamir's approach, using a secret S and a prime number m as (t-1) degree polynomial generated is shown below

$F(X)=(S+a_1X^1+\cdots+a_{t-1}X^{t-1})\bmod m$

Coefficients a1, a2……a t-1 – Are randomly determined from integers within [0, m-1].

Y1=F(1), Y2=F(2).....Y(n)=F(n)

The above equation represents the shadow value Y computed and issued to the participants by the dealer. The set of values present in the shadow are said to be forbidden set. If the participants are less than n, no one in the forbidden set can reconstruct F(x).If the participants are greater than or equal to t then the set of shadows are called qualified set. These shadows are hidden in a cover image which produces a meaningful share which protects the shares from the intruders. Steganography is a process of deriving shadow from a secret S and produce n stego images. In [2] if t participant's stego image is known then the secret and the cover can be reconstructed.

In this present work,the secret image s of size mxm is consider half the size of I in order to not to loose the information .A prime number m is chosen.we further assumed the *i*th secret pixel *si* is a single integer value from $m \times m$ secret image .Than this single integer is coverted into binary and considering two bit as single bit by coverting them into decimal.By applying degree polynomial $F(X)=(S+a_1X^1+\cdots+a_{t-1}X^{t-1})\bmod m$

We are embedding secret image into cover image in order to get stego image and shadow image.By using the equation S=Q+F we are generating number of shares and distributing to different participants. where any t or more of the shares can be collected to recover the secret image, but any t-1 or fewer of them will gain no information about it.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 6, June 2013

III PROPOSED WORK

The flow chart of the proposed work is shown in fig (1)

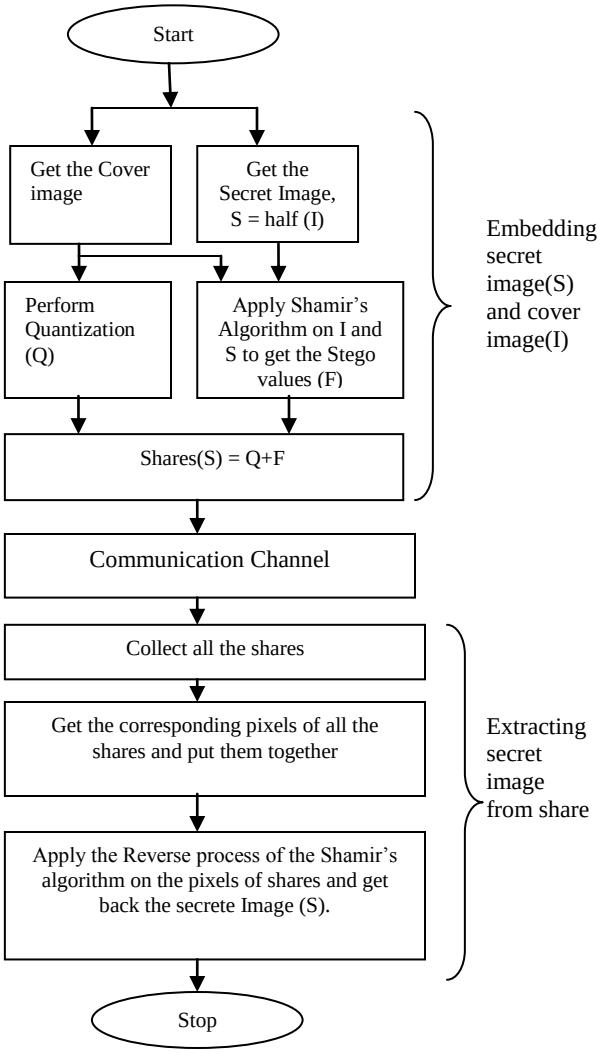

Fig 1
Embedding secret image and cover image

Step 1 :Take input image I and secret image S as half of I.
Step 2: Perform quantization process Q=(p/m)*m on cover image in order to retain actual quality of cover image during reconstruction. Divide the cover image pixel by the prime number m and take the floor value, perform multiplication by prime number on the floor value which gives the quantized value of cover image pixel.
Step 3:Take 2X2 block of I and corresponding pixel of S.Convert S into binary and convert every two bit into decimal.
Stept 4:Apply Shamir's algorithm on I and S F(X)=(S+$a_1X^1 + \cdots + a_{t-1}X^{t-1}$)mod m
Hide the decimal data bit of S into corresponding pixel of cover I ,to get stego and shadow value F Step 5:For number of shares perform ,S=Q+F

Communication channel
stego image is transmitted in the channel to reconstruct secret image with minimum of t shadow, less than t is no use.

Extracting secret image from share
Step 1: collect all shares,for all the shares perform mod(s,m) to get shadow value
Step 2: Apply Shamir's algorithm to get the corresponding pixels of all the shares and put them together in order to get stego image.
Step 3: Take 2X2 block of I and corresponding pixel of S.Convert S into binary and convert every two bit into decimal.
Step 4:By apply quantization process and prime number we are reconstructing secret image.The reconstructed image has better PSNR value.

IV EXPERIMENTAL RESULTS

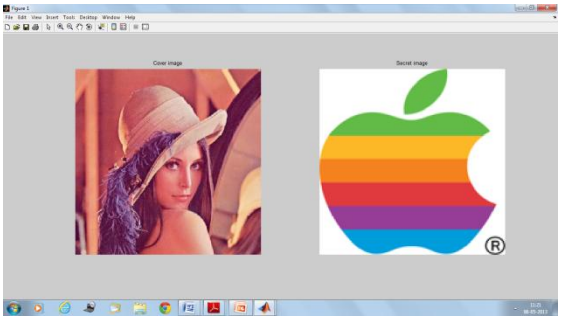

Fig 2.cover image and secret image

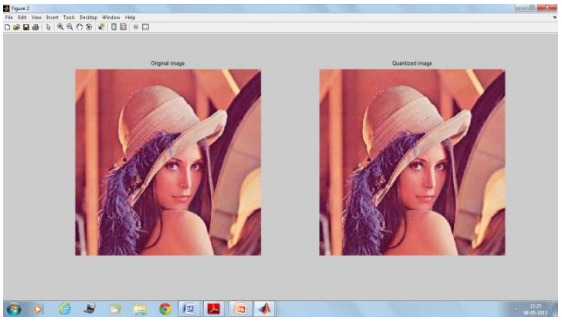

Fig 3.cover image and Quantized image

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 6, June 2013

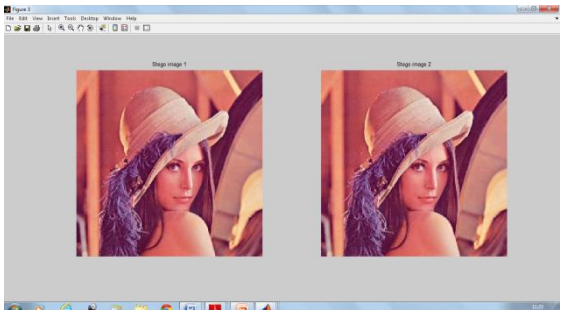

Fig 4.Stego image

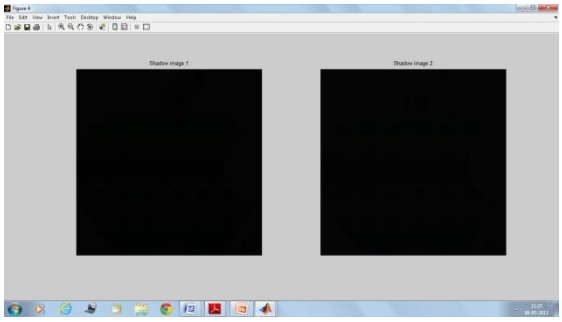

Fig 5.Shadow image

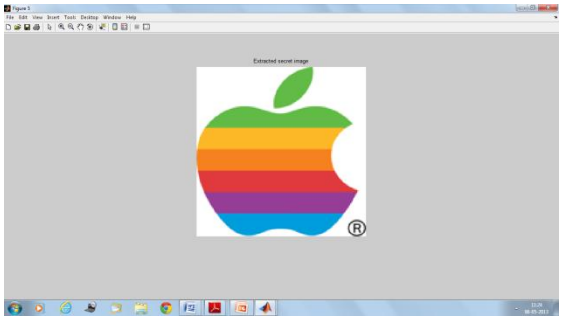

Fig 6.Extracted secret image

V.CONCLUSIONS

In the existing methods, the reconstructed shadows are meaningless and the distortions are large. The proposed reversible image sharing approach for color image reveals the secret image without loss and preserves the cover image. The generated shadows are meaningful with better PSNR value compared with the previous methods. Based on (t, n) threshold scheme, any t authorized recipients can recover the secret by using the reversible process. This methodology can be further enhanced for 3D images and can be used for embedding text and embed speech

ACKNOWLEDGEMENT

I would like to express my deep sense of profound gratitude to my esteemed guide, Prof. Sarojini. B. K, dept of E&C, for her guidance and constant support.I extend my sincere thanks to our Principal,Prof Dr. R.N.Herakal, for the facilities made available during course.I extend my thanks to our HOD, Prof Iddalgi, HOD, dept of E&C,for his kind cooperation. Finally i would like to thank to all those who directly or indirectly supported me .

REFERENCES

[1] L.Jani Anbarasi and S.Kannan. "Secured Secret Color image Sharing With Steganography".
[2] C.-K. Chan, and L. M. Cheng "Hiding data in images ".
[3] Chia-Chun Wu Shang-Juh Kao , Wen-Chung Kuo and Min Shiang"Steganography and Authentication"
[4] Amos Beimel and Benny Chor "Secret Sharing with Public Reconstruction"
[5] Chin-Pan Huang1and Ching-Chung Li2 "A Secret Image Sharing Method Using Integer-to-Integer Wavelet Transform"
[6] DaoshunWanga, Lei Zhanga, Ning Maa, Xiaobo Lib "Two secret sharing schemes based on Boolean operations"
[7] Tzung-Her Chen and Kai-Hsiang Tsao "User-Friendly Random-Grid-Based Visual Secret Sharing "
[8] Chang-Chou Lin, Wen-Hsiang Tsai "Secret image sharing with steganography and authentication
[9] G.R.Blakley "Safegurading cryptopgraphy key".
[10] C.-C. Chan and R.-J. Hwang "Efficient cheater identification method for threshold schemes"