RESEARCHERID
THOMSON REUTERS

[Senthil, 6(4): April 2019] ISSN 2348 – 8034
DOI- 10.5281/zenodo.2652558 Impact Factor- 5.070

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

IMAGE STEGANOGRAPHY BASED ON LSB MATCHING TECHNIQUE USING SECRET SHARING METHOD

S.Azhagu Senthil
Guest Lecturer, Department of Computer Science, Raja Doraisingam Govt. Arts College-Sivagangai

ABSTRACT

Least significant bit (LSB) method is a well-known steganographic algorithm in the spatial domain. LSB drops the visual quality of the image and leads to poor security. To overcome this issue the least significant bit matching revisited steganography was expanded and developed an edge adaptive image steganography. To provide more security for this scheme, this paper provides a combined scheme with (u, v) secret image sharing algorithm. With the additional facility of steganography with authentication and proposes a new algorithm in this paper, which is more secure compared to the previous scheme. This scheme provides four level of security.1) The message is hidden into an image using two keys rotation key (key 1) and the travelling order (key 2) of the algorithm. 2) The (u, v) – threshold function is applied for a batch of n members to share the secret image. Any u or more of v shares can only reconstruct the image consisting of the message. 3) Then the embedding scheme is used to embed each share into camouflage images. 4) The authentication is also provided by the proposed scheme. Thus the scheme is more appropriate for the application where high security and efficiency are mandatory and it can also handle color images with slight modifications.

Keywords: *Covert, Steganography, Secret image sharing scheme, LSB.*

I. INTRODUCTION

Steganography is the mastery of masking information with the help of any appropriate communication medium. Such as text, audio, image, video files. This concealing of information in the medium is done in such a way that no one cannot notice the existence or content of the masked information. The phrase steganography is borrowed from the Greek words “camouflage” meaning “cover” and “grafia” meaning “writing”.

The fundamental idea behind the steganography is to wrap the presence of embedded data. Steganography’s primary roles are un notice ability, robustness (needed for common steganalysis method) and the quantity of embedded information. Steganography is divided into spatial domain and frequency domain. Spatial domain primarily consists of LSB steganography and Bit plane complexity slicing algorithm. Transform domain consists of embedding of secret information into the transform coefficients of the camouflage image.

The rest of the paper is formatted as: section 1 deals with general introduction related to the particular domain, section 2 discussed the related works of image steganography and secret sharing scheme. Section 3 discusses the secret sharing scheme details. Section 4 deals with the proposed methodology. The conclusion is defined as the next section 5.

II. LITERATURE REVIEW

LSB

LSB insertion is a popular stenographic approach. In this embedding procedure, the LSB bits of few or all pixels inside a cover image are replaced by secret bits. The above method introduces some structural asymmetry in the image [5]. Hence identifying the presence of secret becomes easier with the help of steganographic algorithms.

[Senthil, 6(4): April 2019] ISSN 2348 – 8034
DOI- 10.5281/zenodo.2652558 Impact Factor- 5.070

LSB Matching

LSB matching method does a slight alteration to least significant bit method. LSB matching will not directly modify the LSBs of the camouflage image as least significant bit method [8]. If the covert bit is not similar to least significant bit of the camouflage image pixel, at this point either +1 or -1 is added or reduced from the pixel value in the camouflage image. So the simple schemes used for revealing least significant bit method will be unsuccessful at revealing LSBM [3].

LSB Matching Revisited

LSB matching revisited (LSBMR) is not like LSB modification and LSB matching, which uses pixel values individually; LSBMR [4] uses couple of pixel pair as masking unit for hiding the secret bits. The LSBMR hides a secret bit in one pixel and another bit in (odd–even combination) of the both the pixel value. LSBMR uses a pixel pair (pi, pi+1) as a masking unit. In the cover image, after the secret has been hidden, the masking unit will be altered as (p'i, p'i+1) in the stego image which agrees

LSB (p'i) =si, LSB (⌊p'i/2⌋+p'i+1) =si+1.

Function LSB (p) represents the LSB of the pixel value p. si and si+1 are two covert bits to be hidden.

III. SECRET IMAGE SHARING SCHEME

The (u, v) Secret image sharing method was developed by Shamir for safeguarding the secret information [9]. There may be situation where a batch of peoples to share a particular secret information. Shamir developed the model of (u, v) secret sharing method to resolve this issue. Secret is splitted into v share, then shares are distributed to v users where each share alone reveals nothing about the secret information. While any u share can subsequently use to reconstruct the secrets, where u<v. Any u-1 or lesser of shares cannot reveal the secret information.

Edge adaptive image steganography based on LSB matching Technique

Based on this algorithm data embedding stage some parameters must be initialized. This is needed for the preprocessing of information and area selection, and to measure the capacity of chosen area [6]. If the area is sufficient to hide the input message M, at this point data hiding is done in the chosen area. After this step postprocessing is performed to get stego image. If the chosen area is not sufficient, the algorithm will modify the parameter and repeat area selection and capacity measurement till M can be encapsulated totally.

At data retrieval stage the parameters from the stego image retrieved first. Using side information, preprocessing is done and the area used for message hiding is found. Then message M is retrieved using extraction process as described in the algorithm.

This algorithm uses region adaptive method in the least significant bit of the image in spatial domain. The method uses the absolute difference of two adjacent pixel values as criteria for area selection, and use LSB matching revisited as message hiding algorithm [10].

Data Hiding

Step1: First camouflage image of k x n size is divided to equally sized non overlying blocks of Dm x Dm pixels. Then each block is rotated randomly using degrees in the range {0, 90, 180, 270} based on the secret key 1. Resultant image is organized as row vector W using raster scanning and vector W is splitted into non-overlying embedding units with two successive pixel (pi, pi+1).

Step2: The algorithm 1 can hide two secret bits in a unit, for a input message M the threshold L for area selection is calculated has

Data Extraction

In extraction step algorithm1 retrieves the parameters first the size of the block Dm and threshold value L from stego image. After that algorithm 1 follow same procedure as step1 in data hiding. The stego image is divided into non-overlying Dm x Dm blocks and then twisted using random degree based on secret key1. Resultant image is

organized as row vector W'. And we get embedding units by splitting W' to non-overlying blocks which consists of two successive pixels.

IV. PROPOSED METHODOLOGY

The LSB edge adaptive scheme [1] used to hide the message in an image. When the message size increases, using many statistical attacks and steganalysis algorithm, we can notice that the image quality has been decreased. If attackers get access to the two keys i.e. the rotation key (key 1) and travelling order key (key 2) used in this scheme, then it is easy to extract the message from the image. Thus to provide additional security to the message hidden in an image. We combine the above scheme with the (u, v) -threshold secret image sharing method [2].

Data embedding
In data hiding phase first message hidden into a gray scale image of size 256 x 256 using algorithm 1 described previously. All the steps in the algorithm 1 data embedding stage must be followed to insert the message into gray scale image. Before processing the cover image using algorithm 1, we must slightly alter the pixel values of cover image. All the gray scale values greater than 250 (251 through 255) must be restricted to 250. This is to ensure that the algorithm. Each share is embedded in n camouflage images. And each image is delivered to n participants.

Data extraction
In data extraction any k out of n camouflage is collected and the steps in algorithm 2 extraction process is followed to extract the stego image of algorithm 1 (image consisting of message) from k camouflage image and with the help of key 1 and key 2 the algorithm 1 extraction process is applied to the stego image to retrieve the message [7].

V. CONCLUSION

A new scheme for hiding the message has been proposed in this paper by combining two existing algorithm. The proposed system provides high security to the message. The scheme provides four level of security. At first the message is hidden into an image using two keys rotation key (key 1) and the travelling orders (key 2), and then the (u, v) – threshold function is applied for a batch of n members to share the secret image. The embedding scheme and authentication is also provided in the proposed methodology. So, this proposed secret sharing scheme provides more security considerations and efficiency compared with existing methods.

REFERENCES

z *H.Elkam Chouchi and M.A.Makar, 2005. "Measuring Encryption Quality of Bitmap Images Encrypted with Rijndael and Kamkar block ciphers", Twenty Second National Radio Science Conference CNRS (2005), PP.C11, Cairo, Egypt, 2005.*

1. *Giuseppe Mastronardi, Marcello Castellano, Francescomaria Marino, "Steganography Effects in Various Formats of Images. A Preliminary Study," International Workshop on Intelligent dataAcquisition and Advanced Computing Systems: Technology and Applications, pp. 116-119, 2001.*
2. *Lisa M.Marvel and Charles T. Retter, "A Methodlogy for Data Hiding using Images," IEEE conference on Military communication, vol. 3, Issue. 18-21, pp. 1044-1047, 1998.*
3. *Mohammed Ali Bani Younes and Aman Jantan, "A New Steganography Approach for ImagesEncryption Exchange by Using the Least Significant Bit Insertion," International Journal of Computer Science and Network Security, vol. 8, no. 6, pp.247-257, 2008.*
4. *Nawal El –Fishaway, And Osama M.Abu Zaid, Nov 2007 "Quality of Encryption Measurement of Bitmap Images with RC6, MRC6 and Rijndael Block Cipher Algorithms", in International Journal of Network Security, Vol.5, No.3, PP.241-251,. Nov 2007.*
5. *Neil F. Johnson and Sushil Jajodia,1998,, "Steganalysis: The Investigation of Hidden Information," IEEEconference on Information Technology, pp. 113-116, 1998.*
6. *I.Ozturk and I.Sogukpmar, "Analysis and Comparision of Image encryption Algorithms", Transactions on Engineering, Computing and Technology, Vol.3, PP.1305-1313, 2004.*

7. *V.Potdar and E.chang, "Disguising text cryptography using Image cryptography", International Network Conference in plumouth , UK, 6-9, July, 2004.*
8. *P. Subhasri and Dr.A. Padmapriya., "Authentication based Access Control mechanism for Ensuring Privacy of DICOM contents in Public Cloud". Aust. J. Basic & Appl. Sci., 11(10): 128-136, 2017*
9. *M.Van Droogenbroeck and R.Benedett, "Techniques for a Selective encryption of uncompressed and compressed images", in proceedings of Advanced Concepts for Intelligent Vision Systems (ACIVS) Ghent, Belgium, September 9-11, 2002, PP.90-97..*