ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING

National Conference on Advanced Innovation in Engineering and Technology (NCAIET-2015)

Alva's Institute of Engineering and Technology, Moodbidri

Vol. 3, Special Issue 1, April 2015

A Probabilistic model for visual cryptography

Shweta Dodamani

M.TECH in Computer Networks, Shree Devi Institute of Technology, Kenjar, Mangalore, Karnataka, India

Abstract: The visual cryptography (VC) is a secret sharing scheme where a secret image is encrypted into transparencies, by using bit slice algorithm and if stacking of any t out of n transparencies reveals the secret image. If lesser number of transparencies chosen then its not possible to revel the secret.

Keywords: contrast, secret sharing, visual cryptography

I. INTRODUCTION

Visual Cryptography (VC) is a branch of secret sharing. In the VC scheme, a secret image is encoded into transparencies, cryptography is a method of storing and transmitting information in a particular form so that only for those for whom it is intended can read and process image, but the stacking of any or fewer number of transparencies cannot retrieve any information other than the size of the secret image.

Naor and Shamir [1] proposed a -threshold VC scheme based on basis matrices, and the model had been further studied and extended. The probabilistic model of the vc scheme was first introduced by Ito et al.

A. About visual cryptography

Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Original image of 100 by 100 is taken. As it is known that each pixel contains alpha, red, green, blue component. Each Alpha, red, green, blue contains 8bits which is totally of 32 bits ie 4 Bytes. From single pixel we are separating those 4 components and putting it into the new RGBArray1 and RGBArray2 hence it forms six encrypted images.

Basically alpha is used for intensity, brightness etc red is randomized because it forms a carry forward for equal distribution of bits. To extract red component Steps: Extract four msb bits of red component ie one byte, red and put into lsb's of green and blue, red is randomized ie 8bits. Two images per color component ie it forms 6 new images, 2 images for red, green, blue

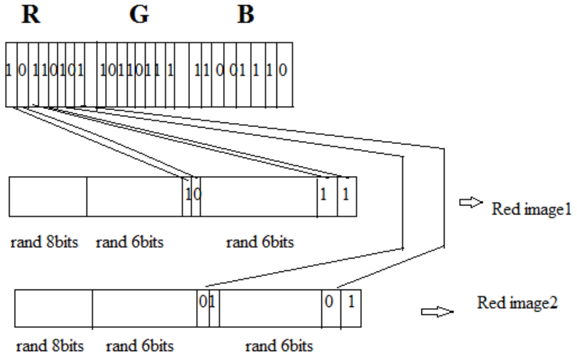
II. EXISTING METHODS

Two methods are used. One is random grids(RGs) introduced by kafri and keren[2] in 1987,other one is basis matrices, RGs is not based on basis matrises.

III. PROPOSED METHOD

This paper proposes two Bit slice algorithms

1.encryption

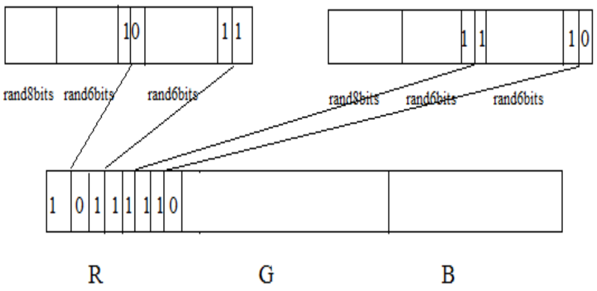


Steps:

- Read the original image.
- gets its RGB into an array
- extract the red component

similarly above method is applied for extracting green and blue component.

2.decryption



i. Read the image pixel into rgbarray

ii. RGBArrays to hold the pixels of images.

iii. shift lsbbyte of even numbered images.

iv. extract four bits of encrypted image.

DOI 10.17148/IJIREEICE

The following are the advantages of using visual cryptography:

- For the security of secrete information.
- Unauthorized users cannot access.
- No risk of hackers.

IV CONCLUSION

The paper proposes a VC scheme with flexible value of n. The future work involves the enhancement of this scheme in area of security in sending information via network.it reduses the threats from hackers, unauthorised users thus providing more security.

REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography," in Proc. Advances in Cryptography (EUROCRYPT'94), 1995, vol.950, LNCS,pp.1–12.

[2] O. Kafri and E. Keren, "Encryption of picturesand shapes by random grids," Opt.Lett., vol. 12, no. 6, pp. 377–379, Jun. 1987.

DOI 10.17148/IJIREEICE