Region Based Cryptography: A Study of Difference Between The Real Image And Image Obtained After RGB

Irfan Jalal Bhat [1], Dr. Raghav Mehra [2], Dr. Amit Kumar Chaturvedi[3]
[1] Research. Scholar, Computer Application, Bhagwant Univeristy Ajmer (India)
[2]Associate Professor & Dean Student Welfare Bhagwant Institute of Technology, Muzaffarnagar (India)
[3] Assistant Professor MCA Departement Govt. Engineering College, Ajmer Rajasthan (India)

Abstract : A region based visual cryptography scheme deals with sharing of image based upon splitting the image into various regions. The main concept of visual secret sharing scheme is to encrypt a secret image into n meaningless share images. It cannot leak any information about the original image unless all the shares are obtained. In this paper we bring the concept what happen when we differentiate the Red , Green and Blue (RGB) colour of image and again obtained the same image after combine the three image i.e Red colour , Blue colour , and Green Colour images. But the last image we obtained after combining all these is slightly differ in quality.

***IndexTerms* - Region Based Cryptography, secrets, sharing, seed, segments.**

I. Introduction

Visual Cryptography schemes usually process the content of an image as a single secret i.e all of the pixels in the secret image are shared using a single encoding rule. This type of sharing policy reveals either the entire image or nothing, and hence limits the secrets in an image to have the same secrecy property. Ran-Zan Wang [1] proposed Region Incrementing Visual cryptography for sharing visual secrets in multiple secrecy level in a single image. The 'n' level RIVC scheme, an image S is designated to multiple regions associated with secret levels, and encoded to shares
with the following features:

a) Each share cannot obtain any of the secrets in S,
b) Any t(2<t<n+1) shares can be used to reveal (t-1) levels of secrets
c) the number and locations of not-yetrevealed secrets are unknown to users,
d) all secrets in S can be disclosed when all of the (n+1) shares are available,

II. Region growing

Region growing is a simple region-based image segmentation method / approaches . It is also classified as a pixel-based image segmentation method / approaches since it involves the selection of initial / start seed points of images. Region growing can be divide into four steps as follow

i. By Selecting seed pixels group in original image.
ii. Select a set of similarity (same) criterion such as grey level intensity or color and set up a stopping rule(norms).
iii. Grow regions by appending to each seed those neighbouring pixels that have predefined(already) properties similar to seed pixels.
iv. Stop region growing when no more pixels met the criterion for inclusion in that region i.e. Size, likeness between a candidate pixel & pixel grown so far, shape of the region being grown.

The benefits of region growing segmentation as .

- Region growing methods can correctly expand the regions that have the same properties / similarities as defined.
- Its gives us a real / original images, which is totally clear view.
- A less number of seed points need to represent the property , then grow the region.so it is quit simple.
- AS number of criteria has chosen to determine the seed ponts.
- The region growing performs well with respect to noise.

The region based segmentation is dividing or partitioning of an image into similar / homogenous areas.
The region based segmenatation contain the terms or schemes as

- Thresholding
- Region Growing
- Classifiers
- Clustering.

III. THE HISTORY OF CRYPTOGRAPHY AS THE HISTORY OF DIGITIZATION

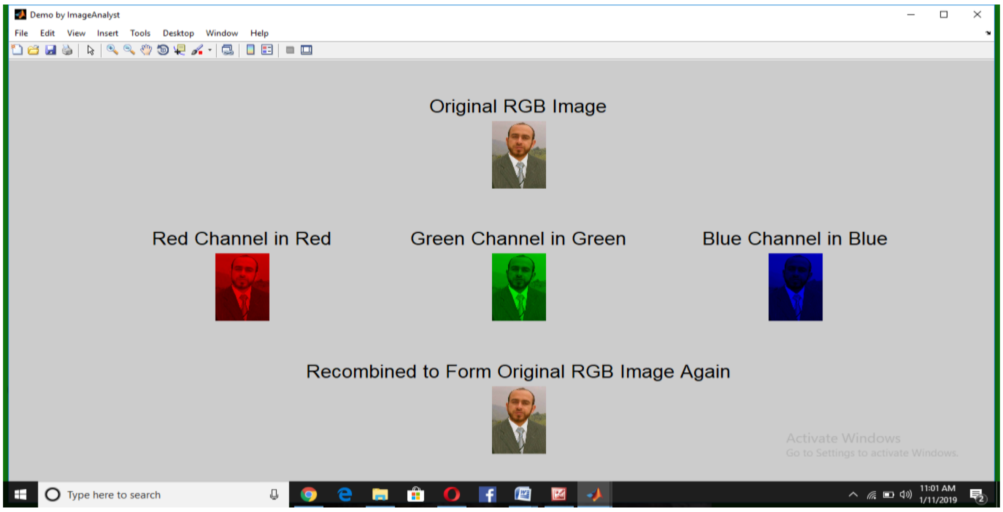
One of the innovations of Morland’s Cyclologica Cryptographica is that it re-quires the use of an Index Digitalis, or digital index, which is a small thimble that fits on one of the digits of the user’s non-writing hand. The point of the index digitalis is inserted into holes aligned next to letters on the wheels. With this digital index secured, the user can spin the disks while simultaneously writing down the ciphered or deciphered messages. Morland’s other machines similarly require the use of what we would today call a “stylus,” a thin, short writing instrument without ink that can be traced across the surface of a device to activate its programming. These machines thus involved the hand in new ways with the composition, storage, retrieval, and analysis of language.2 One of Morland’s contemporaries and the author of the first English cryptography manual, John Wilkins, also described composition methods that challenged the idea of writing, and of text, as only ink on paper. Wilkins described how some of the most important textual artifacts of human history had been ci-phered using a range of methods, like urination, and on unlikely surfaces, like animal skin. Across these stories is acknowledgement of the blurry, even non-existent, line between brainwork and handwork, between creative vision and craftsmanship. The game changers of Wilkins’s cryptographic history, such as the Egyptians who developed hieroglyphics, were simultaneously intellectuals and engineers, and the material form of their messages as important as the con-tent. Their perspective was not the same as Marshall McLuhan’s, who famously claimed that “the medium is the message,” because they still recognized a dif-ference between content and transmission method; rather, they saw the com-position process as necessarily both literary and technical. Cryptographers of the seventeenth century, particularly Morland and his contemporary and fellow Royal Society member Wilkins, broadened the defi-nition of writing, including with it a wide range of material and even immate-rial marking systems. They challenged the notion that writing is only the visi-ble etching of alphabetic characters on a surface; to Wilkins, as he illustrates in his cryptography manual Mercury; Or the Secret and Swift Messenger (1641), writing can use any number of symbolic systems and can manifest on almost any kind of graphic field: in the knots on a string, in the rhythms of fire, in the sound of bells, and in the gestures of the hand. Wilkins is, among other things, credited with one of the first systems of sign language for the deaf, as is yet an-other contemporary cryptographer, John Wallis. Morland imagined the flight of an eagle as a kind of writing, where the wings leave untraceable impressions in the air that can only be deciphered by cryptographic experts like himself (New Method 8). To these early cryptographers, as to a number of contempo-rary natural theologians and philosophers as well, nature was coded. In a sense, they saw code as the necessary precondition for all human experience and ex-pression, so the study of cryptography, even for political or military purposes, was necessarily a humanistic and spiritual pursuit.

IV. METHODOLOGY

The whole process we implemented in MATLAB Coding, First we take an original colour image with name IMG1.jpg which is shown as below

IMG1

After implemented the coding in MATLAB to differentiate the three colour of image i.e. RGB we obtained the images are as under



V. RESULTS

After analyzing the above color image we concluded that the Original RGB Image and the image obtained after Recombined to Form Original RGB Image Again is differ in quality. The quality of image is before is good but after we recombined all the images we obtained that quality of image is low. So in future we have to find the solution of that image we obtained why the quality of the image is lost , which solution is the best for this.

VI. ACKNOWLEDGMENT

We feel grateful to the referees for their valuable suggestions that have helped immensely in preparing the revised manuscript.

REFERENCES

[1] http://www.digitalpolicy.org/going-dark-in-india-the-legal-and-security-dimensions-of-encryption/

[2] Wilfred Diffie and Susan Landau, “Privacy on the Line: The Politics of Wiretapping and Encryption,” MIT Press, (Cambridge, 2007), p. 13

[3] Liddell, Henry George; Scott, Robert; Jones, Henry Stuart; McKenzie, Roderick (1984). A Greek-English Lexicon. Oxford University Press.

[4] Rivest, Ronald L. (1990). "Cryptography". In J. Van Leeuwen. Handbook of Theoretical Computer Science. 1. Elsevier.

[5] Bellare, Mihir; Rogaway, Phillip (21 September 2005). "Introduction". Introduction to Modern Cryptography. p. 10.

[6] Menezes, A.J.; van Oorschot, P.C.; Vanstone, S.A. (1997). Handbook of Applied Cryptography. ISBN 978-0849385230. Archived from the original on 7 March 2005.

[7] Biggs, Norman (2008). Codes: An introduction to Information Communication and Cryptography. Springer. p. 171.

[8] "Overview per country". Crypto Law Survey. February 2013. Retrieved 26 March2015.

[9] "UK Data Encryption Disclosure Law Takes Effect". PC World. 1 October 2007. Retrieved 26 March 2015.

[10] Ranger, Steve (24 March 2015). "The undercover war on your internet secrets: How online surveillance cracked our trust in the web". TechRepublic. Archived from the original on 2016-06-12. Retrieved 2016-06-12.

[11] Blakley, G. (June 1979). "Safeguarding cryptographic keys". Proceedings of AFIPS 1979. 48: 313–317.

[12] Shamir, A. (1979). "How to share a secret". Communications of the ACM. 22 (11): 612–613. doi:10.1145/359168.359176.

[13] "6.5.1 What Are the Cryptographic Policies of Some Countries?". RSA Laboratories. Retrieved 26 March 2015.

[14] Bek, E. (19 May 2016). "Protect Your Company from Theft: Self Encrypting Drives". Western Digital Blog. Western Digital Corporation. Retrieved 8 May 2018.

[15] "DRM". Electronic Frontier Foundation.

[16] "The Padding Oracle Attack - why crypto is terrifying". Robert Heaton. Retrieved 2016-12-25.

[17] "Researchers crack open unusually advanced malware that hid for 5 years". Ars Technica. Retrieved 2016-12-25.

[18] "New cloud attack takes full control of virtual machines with little effort". Ars Technica. Retrieved 2016-12-25.

[19] Examples of data fragmentation technologies include Tahoe-LAFS and Storj.

[20] Burshteyn, Mike (2016-12-22). "What does 'Active Defense' mean?". CryptoMove. Retrieved 2016-12-25.