Advances in Computer Science and Information Technology (ACSIT)
p-ISSN: 2393-9907; e-ISSN: 2393-9915; Volume 6, Issue 2; April-June, 2019, pp. 63-67
© Krishi Sanskriti Publications
http://www.krishisanskriti.org/Publication.html

Automated Seeding: - A Case Study of difference between the Original Image Graph and Graph of Image Obtained after RGB Image

Irfan Jalal Bhat [1], Raghav Mehra [2], 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 Department Govt. Engineering College, Ajmer Rajasthan (India)
E-mail: irfanbhatphd@gmail.com[1], amit0581@gmail.com[2], raghav.mehrain@gmail.com[3]

Abstract—*Now a day's information play a very vital role in every person life. Every person want that his/ her information may kept secret. What so ever he/she done in social sites or elsewhere. When we send a image form one place to other place in-between some attackers or un authorized user attack to steal our information/data. For this different types of methods are used to prevent them .One of them is Image Cryptography. In this paper we take a simple image then draw its graph using Matalab, save it. Again after differentiate the simple image to three colour i.e RED, GREEN, BLUE(RGB) to obtained the image after recombined the RGB and draw the graph of final image and see difference in graph between the simple image and the image obtained after RGB.*

Keywords: *Image Cryptography, Key algorithm, key pixel, RGB Image, Encryption.*

1. INTRODUCTION

With rapid development in internet technology, different types of information can be transferred over internet. Hence there are security issues associated with transmitting high value assets like commercial data, user personal information, banking or transaction data, data related to military. Security of such data transfer must be taken into consideration because hacker can use various methods and steal such high value assets which results in high monetary, social, personal loss. Various schemes are developed to protect such high value assets. Visual cryptography is introduced by first in 1994 Noar and Shamir [2] as a simple way to encrypt and decrypt sensitive data. Visual cryptography is a cryptographic technique which allows visual information (e.g. printed text, handwritten notes and pictures) to be encrypted in such a way that the decryption can be performed by the human visual system, without the aid of computers. Visual cryptography scheme eliminates complex computation problem in decryption process, and the secret images can be restored by stacking operation. This property makes visual cryptography especially useful for the low computation load requirement. In visual cryptography, decryption is done by human visual system hence no need to securely store decryption key. In visual cryptography original image is divided into two parts called as shares. The single share doesn't give any information about original image. When the shares are superimposed together then we can see original image. Adi Shamir in 1979 published an article titled "How to share a secret" [1]. In this article, the following example was proposed to define a typical secret sharing problem: "Eleven scientists are working on a secret project. They wish to lock up the documents in a cabinet so that the cabinet can be opened if and only if six or more of the scientists are present. What is the smallest number of locks needed? What is the smallest number of keys to the locks each scientist must carry? The minimal solution uses 462 locks and 252 keys per scientist." In the paper, (k, n)-threshold scheme was introduced by Shamir to generalize the mentioned problem and formulate it [2]. It can be explained as follows: Let S be the secret to be shared among n parties. A (k, n)-threshold scheme is a way to divide S into n pieces S1,S2, … ,Sn that satisfies the conditions[1]: 1. Knowledge of any k or more Si pieces makes S easily computable. 2. Knowledge of any k−1 or fewer Si pieces leaves S completely undetermined (in the sense that all its possible values are equally likely). Secret Sharing scheme can be applied in different domains. One of the areas that are heavily used this approach is in Visual Secret Sharing (VSS). VSS is a powerful technique that combine the notion of perfect ciphering and Secret Sharing approach. This method uses the idea of hiding secrets within images. These images are encoded into multiple shares and later decoded without any computation. In fact, Visual Secret Sharing approach uses the characteristics of human vision to decrypt encrypted images. The decoding process is as simple as superimposing transparencies, which allows the main secret to be recovered. It would be a great advantage for this method that anyone can physically manipulate the elements of the system, and visually see the decryption process in action without any knowledge of cryptography and without performing any cryptographic computations.

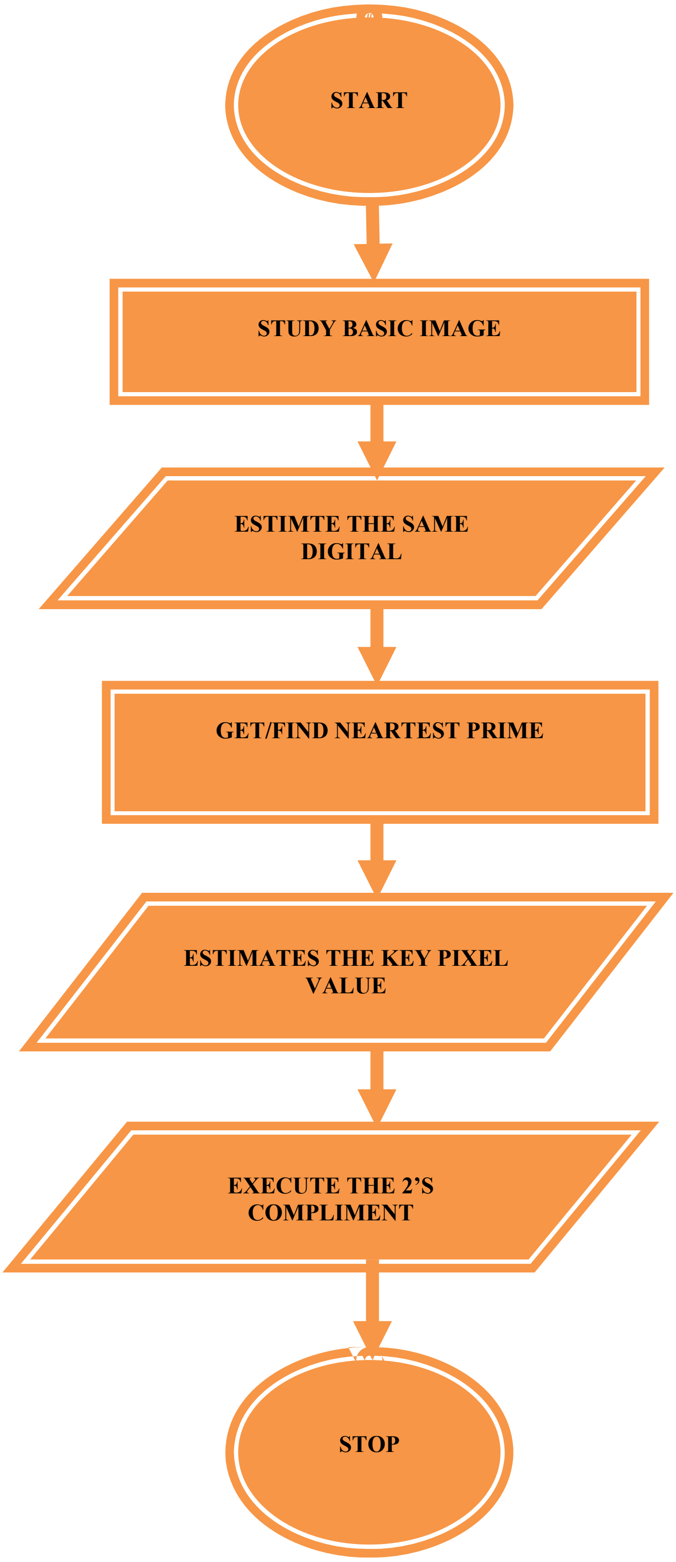
2. LITERATURE REVIEW

Due to lost or steal of information is a big threat in present time. A lot of schemes are used to prevent the information from unauthorized access. In visual cryptography different techniques are used to avoid or illicit used of data (images).In some techniques pixels are used for encryption the images and also used of segment for encryption the images. In segment based visual cryptography segment are used to gives more security to images, as in segmentation uses the seven segment and sixteen display to gives the accurate result .Appropriate techniques are needed to prevent illicit usage of information. Such techniques are called as Secret Sharing Schemes.G.R. Blakley and Adi Shamir independently invented secret sharing scheme in 1979[1]. When it comes to visual information like image, audio and video, then termed as Visual secret sharing scheme. Visual cryptography (VC) is a technique used for protecting image based secrets. Moni Naor and Adi Shamir proposed the basic model of visual cryptography in 1994[2]. In which they stated/ express the idea how to send the image to other recipient without the any information lost/ steal. All shares are necessary to combine to reveal the secret image. There has been a steadily growing interest in visual cryptography. In 2014, Jian Zhang and Yutong Zhang “An Image Encryption Algorithm Based on Balanced Pixel and Chaotic Map” given the A Balanced Pixel Algorithm for Image Encryption. This proposed image encryption algorithm combines the chaos theory and iterative equation, converting the position and the value of each pixel of the original image to finish one loop encryption. In order to obtain a better effect of encryption, the algorithm proposes a method in which the number of encryption times can be defined[7]. In 2016, Ayesha Razia Anha, Dr. T. Bhaskara Reddy “Image Cryptography using Nearest Prime Pixels” comes on the result that This paper focusing on novel key generation using nearest prime pixels. Further different complementary and logical functions are used to improve the secrecy. Finally cipher image is generated with column wise retrieving. This work may be extended with genetic operators and genetic algorithms[8]. In 2017, Najwan AH “Color Images Encryption using Cipher System with different types of Random Number Generator” he concludes in this paper as a simple to implement and effective methods have been proposed for an encrypted image using Linear Feedback Shift Register with maximum input length 100 bits. The register cycles through the maximum number of 2100-1 which it is the output over more seed, Non-Linear Feedback Shift Register using two or more LFBSR which increase the security level and Blum Blum Shub using two large prime random number this make the algorithm is harder for eavesdroppers to know and make security high[9]. In 2019, Hiral Rathod, Mahendra Singh Sisodia, Sanjay Kumar Sharma “Design and Implementation of Image Encryption Algorithm by using Block Based Symmetric Transformation Algorithm (Hyper Image Encryption Algorithm)” concludes that The difference of efficiency between our “Proposed Algorithm” and “Image Encryption Using Block-Based Transformation Algorithm”, “An Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption” is very high approximately 80%. If the security and efficiency is of primary concern then one can use our proposed algorithm. From the above discussion we can clearly see that the proposed algorithm has 70% better entropy of encrypted image any of the other compeering algorithms and hence can be incorporated in the process of encryption of any images. Also, we can see that the “Image Encryption Using Block-Based Transformation Algorithm” and “An Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption” have very less entropy and hence cannot be used for encryption of confidential messages[10].

3. KEY GENERATION ALGORITHM STEPS:-

After analyzing a different research on generation of algorithm we have given some steps are as which are shown as below

I. Firstly, the given image is converted into its equivalent digital pixels.
II. Find nearby prime pixels for each pixel of image.
III. The key values are obtained from result.
IV. Difference between pixel values and nearest prime pixel values.
V. Execute 2’s complement for generated pixels.

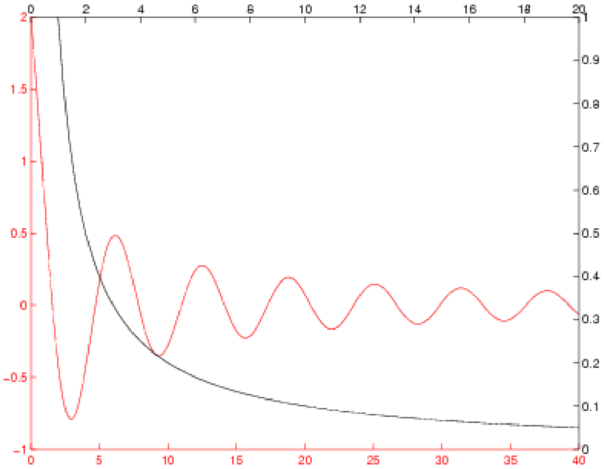


Flow chart showing key generation process

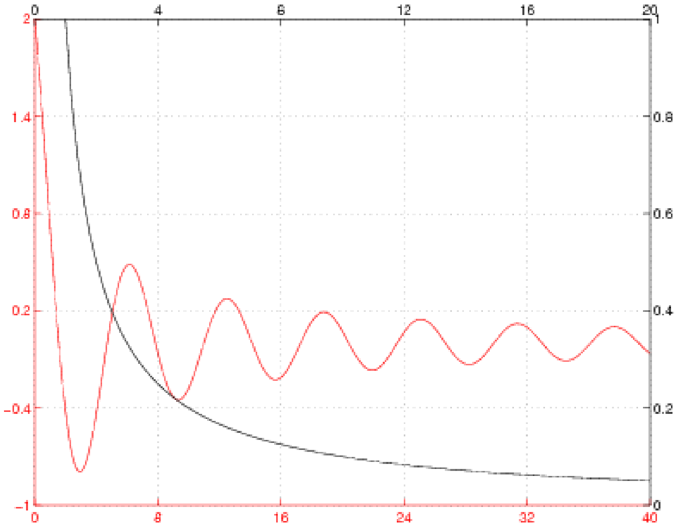
Example for key generation

4. METHODOLOGY

On implemented its MATALAB by finding the a-axis and y-axis of image we find the graph of the first image i.e original image are as



Again when we differentiate the original image into three colours RGB and recombined the three image i.e Red, Green, Blue and obtained the new image. Now we draw of the new image graph as shown as below



5. CONCLUSION

After analysing the graph of both image we have concluded that the slightly difference the both graph as in value and position of axis. The graph obtained from the RGB image is different from the real or original image, this is due the lost of the quality of RGB image. But the image obtained after the RGB is differ in quality of image. The original image is a high quality image everything seen in a image is purely but the image obtained after RGB has low quality as well as the thing in it are not visible purely. Now in future we have to find the lost of quality of the original image and image obtained after RGB. We can also find in future the matrix of the lost the quality of image. Additional different complementary and logical functions are used to obtain better the secrecy. Lastly cipher image is generated with column wise retrieving. This work may be extensive with genetic operators and genetic algorithms

REFERENCES

[1] Blakley, G. R.,“Safeguarding cryptographic keys”, Proceedings of the National Computer Conference, pp: 313–317, 1979.

[2] Naor M., and Shami, A. 1994, Visual cryptography, Eurocrypt’94, Lecture Notes in Computer Science, vol. 950, pp. 1–12.

[3] B.Saichandra.et. al, A New visual cryptography scheme for color images international journal of engineering science and technology vol 2 (6), 2010, 1997-2000.

[4] David Boen, “Segmenting 2d ultrasound images using seeded region growing”, 2006.

[5] T. Monoth and A. P. Babu, “Recursive Visual Cryptography Using Random Basis Column Pixel Expansion”, In Proceedings of IEEEInternational Conference on Information Technology, 2007, pp. 41-43.

[6] Bernd Borchert, Klaus Reinhardt: Abh or- und manipulationssic here Verschl usselung f ur Online Accounts. Patent application DE-10-2007-018802.3, 2007 [Gr07]

[7] Jian Zhang and Yutong Zhang “An Image Encryption Algorithm Based on Balanced Pixel and Chaotic Map” Hindawi Publishing Corporation Mathematical Problems in Engineering Volume 2014, Article ID 216048, 7 pages http://dx.doi.org/10.1155/2014/216048

[8] Ayesha Razia Anha, Dr. T. Bhaskara Reddy “Image Cryptography using Nearest Prime Pixels” Int. J. Advanced Networking and Applications Volume: 08 Issue: 02 Pages: 3026-3028 (2016) ISSN: 0975-0290

[9] Najwan AH “Color Images Encryption using Cipher System with different types of Random Number Generator” International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 5, Issue 5, May2017

[10] Hiral Rathod, Mahendra Singh Sisodia, Sanjay Kumar Sharma “Design and Implementation of Image Encryption Algorithm by using Block Based Symmetric Transformation Algorithm (Hyper Image Encryption Algorithm)” International Journal of Computer Technology and Electronics Engineering (IJCTEE) Volume 1, Issue 3,2019

[11] FA Behrouz, Data Communications and Networking, ed. 5. 2012: McGraw-Hill 2012.

[12] PP Dang, PM Chau, Image Encryption for Secure Internet Multimedia Applications. IEEE Trans. Consumer Electronics 2000; 46:395-403.

[13] S Shrija, HA Mohammed, Securing Medical Images by Image Encryption using Key Image. International Journal of Computer Applications 2014; 104: 30-34.

[14] K Vishal, PT Surya, et al. Two Level Image Encryption using Pseudo Random Number Generators. International Journal of Computer Applications 2015; 115:1-4.

[15] BK Arihant, T Namita, Image Encryption using Pseudo Random Number Generators. International Journal of Computer Applications 2013; 67:1-8.

[16] L Suhad, HA Najwan, Color Image Encryption using Random Password Seed and Linear Feed Back Shift Register. Journal of Al-Nahrain University 2011; 14:186-192.

[17] W Mark, Web's random numbers are too weak, researchers warn. Technology correspondent, BBC News in Las Vegas 2015.

[18] R Andrew, S Juan, et al. Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. National Institute of Standards and Technology Special Publication 2010; 131.

[19] KE Donald, Pseudo randomness. The Art of Computer Programming 2009; 2.

[20] K Choi, KCT Jung, The importance of PN Sequences in the Design of Spread Spectrum Systems. IEEE Trans. Commun 2001.

[21] S William, Cryptography and Network Security: Principle and Practice, ed. 7th. 2017: Prentice Hall. 752.

[22] QRS Gamil, TN Sanjay, Encrypting Image By Using Fuzzy Logic Algorithm. International Journal of Image Processing and Vision Sciences 2013; 2.

[23] EL Lehmann, C George, Theory of Point Estimation ed. 2, New York: Springer 1998; 590.

[24] G Mohammed, Q Huynh, Scope of validity of PSNR in image/video quality assessment. IEEE Xplore 2008; 44:800-801.

[25] MJ Alfred, OVC Paul, et al. Handbook of Applied Cryptography, ed.5, CRC Press Inc. 2001; 816.