A Survey on Secret Image and Data Sharing Based on Encrypted Pixels

Harshitha S[1], Mrs.Shwetha K S[2], Dr. Anandhi R J[3]

[1]Student, [2]Senior Assistant Professor, [3]HOD
Department of Information Science Engineering,
New Horizon College of Engineering
Outer Ring Road, Marathalli, Bengaluru- 560 103

***Abstract*: Data security and protection is one of the essential necessities in the realm of data and communication technology. Securing the data has become a critical issue. These days, picture containing private and secret data are broadly conveyed through open channels. What's more, consequently it had turned out to be progressively essential to gadgets and other device to secure such information or images from purposeful or unexpected interruption.**
In order to provide a secure method to protect important data and image, visual secret sharing (VSS) scheme is being proposed and variety of Techniques such as image Steganography, copy detection, Encryption, Decryption and algorithms like Linear equation and random grid including XOR operation is utilized.

Keywords: Image Steganography, Linear equation, Random grid, XOR operation, copy Detection, Encryption and decryption

I. INTRODUCTION

Data security and protection is one of the essential necessities in the realm of data and correspondence innovation. Cryptographic strategies and instruments assume a major job in making the data secure. In perspective on the remarkable increment in the data stream over the system, secure correspondence has turned into a basic issue. These days pictures containing private and classified data are broadly imparted through open channels and subsequently it has turned out to be progressively critical to gadget secure techniques to shield such data from purposeful or accidental interruption. As an answer for secure picture sharing issue, Visual Secret Sharing (VSS) scheme, that established the framework of visual cryptography. VSS scheme is a cryptographic strategy reasonable for applications to picture information. In this paper, a secret image is deteriorated into ($n > 1$) good for nothing shares. Stacking ($k \leq n$) more shares uncovers the importance of secret. The most essential component of this strategy is that the decoding does not require any intricate calculation and depends just on the human visual framework. This plan is otherwise called (k, n) VSS plot, as any arrangement of not as much as k shares does not uncover any data about the mystery.

The visual secret sharing (VSS) scheme is a creative and ensured picture sharing scheme. In secure sharing plan it has a few constraints, First every shares of secret picture is bigger on the grounds that to improve the proficiency and looking after security. Furthermore a secret plot utilizes a arbitrary piece to convey among irregular bits. It endured from couple of downsides. To begin with, every pixel of a picture was spoken to by more than one pixel in an offer of picture. Each picture is separated into offers of higher size, require high memory, unscrambling process experiences low differentiate.
Data Encryption is the process of translating the text data or images into something that appears to be a random and meaningless (ciphertext). Data Decryption is the process of converting those random and meaningless text back to proper image and data. To encrypt the smaller amount of data, symmetric encryption is used. Both encryption and decryption uses symmetric key. To decrypt a particular ciphertext, the encrypted key should only be used.

Matrix Laboratory is a platform which is utilized for solving numerical and scientific problems. It is a restrictive programming language developed by MathWorks, functions, matrix manipulations and data plotting, algorithm implementation, user interface creation and interfacing with programs written in programming language such as C++, C, java etc. The IPT is a collection of capacities that extend the numeric computing environment.it gives thorough arrangement pf reference-standard algorithms and workflow applications for image processing, visualization, analysis and algorithm development. It can be utilized to perform image enhancement, image segmentation, geometric transformation, noise reduction, image registration and 3D image processing operations. Huge number of IPT functions support code generation for desktop prototyping and embedded vision system development.

Image processing is the technique which converts image into digital/computerized format and perform tasks on it to get an improved image or concentrate some valuable data from it. Changes that happen in images are typically performed naturally and depend on well-designed algorithms. It is a multidisciplinary field, with commitments from various parts of science including arithmetic, material science, optical and electrical designing. Besides, it covers with different zones, for example, design acknowledgement, AI, machine learning and human vision researches.
Computerized cameras and camcorders, top-notch TVs, screens, DVD players, individual video recorders and mobile phones are well known buyer gadgets use image processing.

II. LITERATURE SURVEY

P.S.Revenkar, Anisa Anjum, W .Z. Gandhare introduced a Visual Cryptographic Schemes on the basis of number of secret images, pixel enlargement, image Format and sort of share generated. Taking restricted information measures such as limited bandwidth and consideration storage of two criteria pixel enlargement and range of shares encoded is of significance. Smaller pixel enlargement ends up in smaller size of the share which scale back the storage capability and network transmission bandwidth. coding multiple secret images into a similar share images need less overhead whereas sharing multiple secrets. significant shares avoid attention of hacker considering the protection problem over the communication channels. Unmeaning shares increase the interest of hacker. To satisfy the demand of today's multimedia system info gray and color image format ought to be encoded by the schemes. Alternative performance measures like accuracy, security and contrast, computational complexity that have an efficiency of visual cryptography are also discussed.

Jithi P V, Anitha T Nair proposed an advanced Watermarking method that is utilized to create significant meaningful shares. The secret image are watermarked with various spread images and are transmitted. At the receiving side the spread image is extricated from the shares and stacked one by one which uncovers the secret image logically. In this paper,this scheme gives a progressively productive approach to cover up images in various meaningful shares giving high security and recouped with high contrast.

Adi Shamir implemented Secret Sharing Scheme (SSS) which is a threshold scheme that utilizes the concept of polynomial interpolation. The scheme reveals the mystery of sharing the images synchronously or asynchronously. At the point when shares are revealed synchronously all the images are uncovered at same time. At the point when shares are uncovered asynchronously, images uncover their shares each one in turn. The threshold scheme (n, t), Let S be some secret information where the secret can be split into number of pieces and combined together to generate original secret. The pieces leave undermined when there is less than n. The scheme contains Central authority which gives the share of the participants and able to reconstruct the secret from their shares accomplished by given each participants or more can together reconstruct the secret.

Thien – Lin introduced a (k, n) Threshold based Secret Image Sharing Scheme (SISS) which is extended from Shamir's polynomial approach. The paper suggested instead of taking random numbers (k-1), k image pixels would be picked up. At first read the secret image S, this scheme suppresses all the pixel value larger than 250 are taken constantly truncated to 250, Sequentially the distinct k pixels of S image which are not taken are already under polynomial equation of order(k-1). Then preceding the generation of n pixels for n shadow images. In this paper the steps are repeated until all pixels of images not get covered and n shadow images are distributed among participants. The secret image reconstruction is being proposed by collecting any distinct k shadow images which are not yet used pixel from each shadow image using Lagrange's interpolation formula to get the coefficients of polynomial functions f(x). These coefficients sequentially form a permuted image and the pixels of permuted image inversely gets the original image back in form. Thien and Lin also proposed lossless image secret sharing scheme which helps the pixel value to keep in track that are greater than 250.

Ching-Nung Yung introduced Visual Cryptography i.e Visual Secret Sharing (VSS), Encrypted techniques and Secret Image Sharing scheme which can easily avoid the pixel expansion problem as well as it requires no codebook design. In this paper, a new threshold based on VSS scheme aiming to improvise the visual quality of previewed image that are presented. This scheme is compared with previous schemes and can gain better visual quality in the reconstructed images including the (k, n) threshold and have secure mechanism to protect against the unauthorized data access, dissemination of many sensitive information. The paper makes sure that the image data protection, image-based authentication techniques offer efficient solutions for controlling how private image and data could be available only to secret people, contrast enhancement techniques, color-image visual cryptography, alignment problem for image shares, steganography and authentication. These essential design of system are used to manage certain sensitive data like medical records, financial transaction and electronic voting system which are addressed in this paper.

III. PROPOSED SYSTEM

A strategy based on a system of linear equations with secret keys such as coefficients is used to divide a secret image into sub images of smaller size. Then the conception of random grid is applied to the sub images for construction of the shared pictures. Even an approximate guess of encryption key is possible to reveal the secret information and even though attacker do not have the encrypted keys, image can be revealed partly if random grid is simply XOR'ed with encrypted sub images.
The present scheme takes care of issues that are mentioned above, it makes more secure on one hand and guessing of the coefficients under liner equation is more difficult, then the random grid to randomize the coefficient values with XOR operation is applied to make the shared images more secure and beneficial.

CONCLUSION AND FUTURE WORK

Information security and privacy as become one of the major necessities in the world of communication and information technology. Cryptographic methods containing Encryption and decryption tools play a big role in making the data and images secure. In the view of unprecedented increase in information flow over securing communication and network has become a critical issue. Nowadays confidential and private information are widely communicated in open channels so it is important to protect from intentional or unintentional intrusions.

Several surrogate methods based on image processing on Linear equation and random grid with XOR operation has been Proposed for improving the security of important data and images. The proposed methods were applied to different scenarios for copy detection, encryption and decryption techniques. The most important feature of this technique is that the decryption do not require any complex computation and only depends on human visual system and VSS scheme, of any set less than k shares do not reveal any information about the secret.

Proposed strategy utilizes simple linear equation and reliance among their coefficients. Since the coefficients of liner equations are employed during encryption that are randomized for every pixel square using the random grid or irregular framework, it is unrealistic to figure the coefficients. The method is proposed for single secret sharing of important data and images which is accurate and efficient.

REFERENCES

[1] P.S.Revenkar, Anisa Anjum, W .Z. Gandhare, Department of Computer science, Mumbai university, K.J.Somaiya college of Engg, Mumbai, India, International Journal of Infinite Innovations in Technology|ISSN:2278-9057 IJIIT|Volume-III|Issue-I|2013-2014 July|Paper-11 Reg. No.:20140611|DOI:V3I1P11
[2] Jithi P V, Anitha T Nair, Engineering and Technology, 2 nd International Conference on Current Research Trends in Engineering and Technology © 2015 IJSRSET | Volume 4 | Issue 5 | Online ISSN : 2394-4099|Print ISSN: 2395-1990 |
Adi Shamir, Department of Applied Computer Science The University of Winnipeg 515 Portage Avenue, Winnipeg, MB, Canada
[3] Adi Shamir, Department of Applied Computer science, The University of Winnipeg 515 Portage avenue. Winnipeg,MB, Canada, IEEE International Conference on Multimedia and Expo,July 2016 with 202 Reads, Fifth International Conference on Computing, Communications and Networking Technologies (ICCCNT).
[4] A.Shamir's, Computer science Engineering, Parul Institution of Engineering and Technology, Vadodara,Gujarath,India| IJSRSET 2016 |Volume 2|issue 3|Print ISSN:2395-19990.
[5] A. Shamir, "How to share a secret",. ACM, Commun, vol. 22, no. 11, pp. 612-613, Nov. 1979
[6] Thien – Lin , Department of Engineering and Technological Studies, University of Kalyani, Kalyani 741 235, India. Academy of Technology, West Bengal University of Technology, Hooghly 712121, India, Egyptian Informatics Journal-2015
[7] Thien and Lin's, IEEE Xplore Digital Library| DOI: 10.1109/ACCESS.2018.2811722
[8] Ching-Nung Yung, Department of Computer Science and Information Engineering, National Dong Hwa University, Hualien County 97401, Taiwan , Digital Object Identifier 10.1109/ACCESS.2018.2811722
[9] Y.-Y. Lin and R.-Z. Wang, ''Scalable secret image sharing with smaller shadow images,'' IEEE Signal Process Lett., vol. 17, no. 3, pp. 316–319, Mar. 2010.