Natural Image Sharing With Data Hiding and Extraction by Carrier Media: A Review

Ms. Snehal R.Awatade, Prof. A. D. Gawande

***Abstract*— To maintain the secrecy and confidentiality of pictures may be a spirited space of analysis, with 2 completely different approaches being followed, the primary being encrypting the photographs through encoding algorithms victimization keys, the opposite approach involves activity knowledge victimization data activity algorithmic rule to keep up the photographs secrecy. A content owner encrypts the initial image victimization AN encoding key, and a information-hider will introduce extra data into the encrypted image employing a data-hiding key though' he doesn't grasp the initial content. With AN encrypted image containing extra information, a receiver could 1st decode it consistent with the encoding key, and so extract the embedded information and recover the initial image consistent with the data-hiding key.**

Keywords— Cover image, data hiding, data extraction, Image encryption, Image decryption and Data recovery.

I. INTRODUCTION

Cryptography could be a technique for securing the key info. Sender encrypts the message victimization key and so sends it to the receiver. The receiver decrypts the message to urge the key info. Cryptography focuses on keeping the content of the message secret where as data hiding concentrates on keeping the existence of the message secret [1]. Knowledge concealing is that the different technique for secured communication. Knowledge concealing involves concealing info thus it seems that no info is hidden the least bit. If an individual or persons views the item that the data is hidden inside he or she is going to haven't any concept that there's any hidden information, thus the person won't commit to decipher the data [2]. Knowledge concealing is that the method of concealing a secret message among cowl medium like image, video, text, audio. Hidden image has several applications, particularly in today's trendy, advanced world. Privacy and secrecy could be a concern for many individuals on the net. Hidden image permits for 2 parties to speak on the QT and covertly.

Manuscript received November 05, 2014.

Ms. Snehal R.Awatade, Master of Engineering Scholar, Computer Science and Engineering Department, Sipna college of engg and technology Amravati, India

Prof. A. D. Gawande, Head of CSE Department, Computer Science and Engineering Department, Sipna College of engg. and technology,Amravati, India

The strength of knowledge concealment gets amplified if it combines with cryptography. The terminologies employed in knowledge concealment square measure cover-image, hidden image, secret message, secret key and embedding algorithmic rule. Cover-image is that the carrier of the message like image, video or audio file. Cover-image carrying the embedded secret knowledge is that the hidden image. Secret message is that the data that's to be hidden in a very cowl image. The key secrets won't to insert the message betting on the concealment algorithmic rule [2]. The embedding algorithm is that the way that is employed to insert the key data within the cowl image.

The security of the transformation of hidden knowledge may be obtained by 2 ways: secret writing and knowledge concealment. a mixture of the 2 techniques may be wont to increase the info security. In secret writing, the message is modified in such some way in order that no knowledge may be disclosed if it's received by associate degree wrongdoer. Where as in knowledge concealment, the key message is embedded into a picture typically referred to as cowl image, then sent to the receiver World Health Organization extracts the key message from the duvet message. Once the key message is embedded into cowl image then it's referred to as a hidden image [6]. The visibility of this image mustn't be distinguishable from the duvet image, in order that it nearly becomes not possible for the wrongdoer to find any embedded message.

II. LITERATURE SURVEY

Fridrich et al. (2001) [3], planned the reversible knowledge embedding methodology for the authentication purpose therefore the embedding capability of this methodology is low. To separate the info extraction from image decoding, Zhang empty out house for knowledge embedding within the plan of press encrypted pictures [4], [5].

An encrypted binary image are often compressed with a lossless manner by finding the syndromes of low-density parity-check codes, a lossless compression method for encrypted gray image using progressive decomposition and rate-compatible punctured turbo codes is developed in [4]. W. Liu, W. Zeng, the lossy compression methodology bestowed in [5], Associate in Nursing encrypted grey image are often expeditiously compressed by discarding the to a fault rough and fine data of coefficients generated from orthogonal remodel. Once having the compressed knowledge, a receiver could reconstruct the principal content of original image by

retrieving the values of coefficients. The computation of remodel within the encrypted domain has additionally been studied X. Zhang [8].

W. Liu, W. Zeng projected, once the key knowledge to be transmitted area unit encrypted, a channel supplier with none information of the cryptological key could tend to compress the encrypted knowledge because of the restricted channel resource, a lossless compression methodology for encrypted grey image exploitation progressive decompose and rate compatible turbo codes is developed in [5].

The method in [6] compressed the encrypted LSBs to vacate space for extra knowledge by finding syndromes of a parity-check matrix, and also the facet data used at the receiver facet is that the spacial correlation of decrypted pictures.

A novel methodology for RDH in encrypted pictures, that we tend to don't vacate space when encryption as drained [7], however reserve space before encryption. In that, we tend to 1st empty out space by embedding LSBs of some pixels into different pixels with a standard RDH methodology then write in code the image, therefore the positions of those LSBs within the encrypted image may be accustomed introduce knowledge. In ways of [6]–[7], the encrypted 8-bit gray-scale pictures area unit generated by encrypting each bit-planes with a stream cipher.

Research has centered on gray-level and color secret pictures to develop a easy VSS theme that adds cowl pictures into the purposeless shares. To share digital pictures, VSS schemes use digital media as carriers that makes the looks of the shares a lot of variable and a lot of user friendly. Many papers investigated meaning halftone shares and emphasized the standard of the shares quite the standard of the recovered pictures. These studies had serious aspect effects in terms of component enlargement and poor show quality for the recovered pictures, although the display quality of the shares was enhanced. Hence, researchers build a trade-off between the standard of the shares, the quality of the recovered pictures, and also the pixel expansion of the pictures. In another research branch, researchers used steganography techniques to cowl secret pictures in cover pictures. Steganography is that the technique of concealment data and creating the communication invisible. during this way, nobody World Health Organization isn't concerned within the transmission of the data suspects the existence of the data. Therefore, the hidden data and its carrier will be protected. Steganography has been wont to hide digital shares in VSS schemes. The shares in VSS schemes square measure embedded in cowl pictures to createstego-images. Though the shares square measure hid entirely and the stego-images have a high level of user friendliness, the shared data and also the stego-images stay intercepted risks throughout the transmission part .Recently, Chiu et al. tried to share a secret image via natural pictures [11]. This was a primary arrange to share pictures via natural images; but, this work might suffer a problem—the textures of the natural pictures may well be disclosed on the share. Moreover, written pictures cannot be used for sharing pictures within the previous theme.

Visual cryptography may be a widespread answer for image secret writing. Victimization secret sharing ideas, the secret writing procedure encrypts a secret image into the shares that square measure noise-like secure pictures which may be transmitted or distributed over Associate in Nursing untrusted communication. victimization the properties of the HVS to force the popularity of a secret message from overlapping shares, the key image is decrypted while not further computations and any data of cryptography[12].

Guiqiang Chen [II] has bestowed Associate in Nursing economical Color Image Sharing technique supported Lagrange's Interpolating Polynomial. Chen's theme [II] uses Lagrange's Interpolation Polynomial for secure transmission of a color image. it's proposed that the p share images of the key image were made by compressing, substitute, cryptography and destroy to the key image and every share image is hidden in a standard image known as stego image; thus, less attention paid by the malicious users, if Associate in Nursing malicious users gets the standard image (which is containing the share information)[13]. The scale of every stego image is l/q of the key image. To recover the original secret color image letter of the alphabet shadow pictures out of p square measure used.

From thousands of year our ancestors square measure victimization steganography. For eg., the sender hide messages at intervals wax tablets, on messenger's body, on paper written in invisible inks, on envelopes lined by the stamp etc. fashionable steganography hides the secret image into pictures, audio, video, text.

In 1994, Naor & Shamir, projected visual cryptography theme. During this secret image is split into specifically 2 shares & each shares are needed for the secret writing method. In this, the shares generated are nonsensical and is employed for black & white pictures solely.

In 1996, Ateniese, Blundo & Stinson projected extended visual cryptography schemes that contain substantive share pictures. The (2,2) EVC theme projected during this needed enlargement of 1 picture element within the original image to four sub pixels which may then be elite to provide the desired pictures for every share.

Until the year 1997, visual cryptography schemes were applied to solely black & white pictures. 1st colored visual cryptography theme was developed by Verheul & Tilborg. The disadvantage of this theme is that they use nonsensical shares to cover the key image & the standard of the recovered plain text is dangerous.

In 2002, Nakajima & Y. Yamaguchi , projected a system that take a three photos as associate degree input & generates 2 pictures that correspond to 2 of the three input photos. The third image is recovered by stacking the 2 output pictures along. While the previous researches chiefly specialize in binary pictures like text pictures this paper uses the EVC theme appropriate for natural pictures like photography.

In 2003, Hou projected another color VC theme. Supported the halftone technique & color decomposition, it decomposes the secret image into 3 colors C, M & Y. By manipulating the three colors values, the color pixels within the secret image are often portrayed[14].

In 2008, H. chu wu, Hao-cheng wang & Rui-wen yu[14] , proposes a color visual cryptography theme that generate substantive shares. These substantive shares won't attract the eye of hackers. The projected theme uses the halftone technique, cover coding tables & secret coding table to

get two meaningful shares. the key image are often recovered just by stacking the 2 meaningful shares together.

In 2010, Q. Chen, X. Lv, M. Zhang, Y. Chu , projected associate degree extended visual cryptography theme with multiple secrets hidden. Meaningful shares are generated by using the principle of contrast & multiple secret images may be hidden by changing the overlapping angle of the shares. This scheme may also apply to paint image. The theme is straightforward & effective & shares even have enough security level.

In 2012, M. Kamath, A. Parab, A. Salyankar, S. Dholay, proposes a new visual scheme for color images. The projected theme makes use of Jarvis error filter, a key table & specialized tables for coding.

Image Encryption: The main plan within the image secret writing is to transmit the image firmly over the network so no unauthorized user will able to decipher the image[15]. The image information has special properties like bulk capability, high redundancy and high correlation among the pixels that imposes special needs on any secret writing technique.

Prior add the realm of knowledge retrieval within the encrypted domain centered on text documents. Song et al. , Brinkman et al. , and Boneh et al. Explored Boolean search to spot whether or not a question term is gift in associate degree encrypted text document. Swaminathan et al. projected a framework for rank-ordered search over encrypted text documents, so that documents may be came within the order of their relevance to the question term. Therein work, many protocols are studied to handle totally different operational constraints like different communication value allowed performing the secure search. Secure text retrieval techniques may be applied to keyword primarily based search of image information. However, keyword search depends on having correct text description of the content already on the market, and its search scope is conned to the prevailing keyword set. In distinction, content-based search over associate degree encrypted image information provides additional exibility, whereby sample pictures are bestowed as queries and documents with similar visual content within the information are known. An rising space of labor associated with confidentiality preserving image retrieval is secure signal process, which aims at activity signal process tasks whereas keeping the signals being processed secret. Erkin et al. [16] provided a review of connected science primitives and a few applications of secure signal process in information analysis and content protection. However, applying science primitives to the task of content-based image retrieval isn't easy. Effective image retrieval usually depends on evaluating the Similarity of 2 documents exploitation the space between their

Visual options, like color histograms, form descriptors, or salient points. By design, ancient science primitives don't preserve the space between feature vectors after cryptography. Given the a lot of larger information volume for image information than that of text and different generic information, efficiency and measurability are crucial for image retrieval however will be tough to attain exploitation science primitives alone. Another work by Shashank et al. addresses the matter of protective the privacy of the question image once looking out over public information, wherever the photographs within the information are not encrypted. By fittingly formulating the question message and response message throughout multiple rounds of communication between the user and also the server, the server is made oblivious to the particular search path and therefore unaware of the question content.

The chaotic supply map primarily based image coding technique planned by N.K. Pareek, Vinod Ptidar and K.K.Sud[17] presents associate degree formula that utilizes 2 chaotic supply maps associate degreed an external key of eighty bits. To encrypt the pixels of a picture eight differing kinds of operations are used. Another chaotic supply map technique are planned by Mrinal Kanti Mandal, Gourab Dutta Banik, Debasish Chattopadhyay and Debashis Nandi. This method was used on the gray level wherever the XOR operations and constituent shuffling of the image are wont to confused and diffuse the constituent worth and the constituent position. In the higher than techniques, the whole image is encrypted and decrypted when, that could be a huge overhead just in case of storage and retrieval of enormous set of pictures, in a image database or transmission of pictures over giant associate degree insecure channel. Conjointly the loss of even a little a part of the encrypted images leads to bigger distortion within the decrypted image. This is thanks to the actual fact that the part of the encrypted image which is distorted constitutes pixels that may be scattered in the decrypted image.

Alfre Jo Diamond State Santk et.al planned visual cryptography schemes during which 2 picture elements mix in varied discretionary ways that and so analyze the pixel growth. during this theme every share has some data of the key image however solely the desired n variety of shares can reconstruct the image. the mixture of shares will be done by victimization any Boolean operate like “OR” “XOR” etc. Chin-Chen Chang Jiang et.al has planned a good and generalized theme of concealing a color image. This theme uses a color index table to cover and recover the image. In ill a secret image, terribly little memory area and straightforward computations are needed. Chin-Chen Chang Jiang et.al has planned colored visual cryptography schemes supported changed visual cryptography. This uses only a few further computations to cover a colored secret image into some shares. Size of the shares and therefore the implementation complexness during this theme depends on the quantity of colors showing within the secret image. a lot of economical approach is to cover a grey image (256-colors) in numerous shares. The dimensions of the shares are fastened and don’t vary with the quantity of colors showing within the secret image. The fresh planned theme has the advantage of low computation and it additionally avoids the drawbacks of the previous approach, it's much appropriate for today’s demand of low power. Stelvio Cimato et.al [18] has planned another visual cryptography theme that permits the encryption of a secret image into n shares that are distributed to the participants; specified solely qualified subsets of participants will visually recover the key image. In colored threshold visual cryptography schemes the key image contains pixels from a given set of c colors. This paper shows the c-color (k, n)-threshold visual cryptography schemes. Zhi Zhori and Gonzalo et.al has planned a theme during which the key

image, SI is encoded into n shares of random patterns. This theme decodes the key image by superimposing the desired variety of shares onto transparencies; however no secret data will be obtained from the superposition of an impermissible set. This theme is mathematically secure. Wei-Qi Yan, couple Jin planned the applications of Visual Cryptography on print and scan pictures. There ar several difficulties in printing or scanning the key image shares. the most reason for this can be the issue of use in follow. The shares ar written onto transparencies and so has to position them. However it's not terribly straightforward to try precise superposition attributable to the fine resolution and therefore the printing noise. There should be some criteria to search out the alignment of all the shares so as to avoid any issue in superimposition. This paper uses Walsh remodel to insert marks all told the shares to search out the alignment position of those shares. Experimental results shows that it's terribly helpful in print and scan applications. Chih-Ming Hu and Wen-Guey Tzeng planned the tactic of detection the cheating bar in visual cryptography.

Chang-Mok Shin, Dong-Hoan Seo, Kyu-Bo Chol, Ha Wmn Lee, Associate in Nursingd SmJmng Kim projected an rule which was construction type of image encoding victimization binary part exclusive OR operation and image dividing technique. The same gray level multi-level image is split into binary pictures. Then binary pictures is regenerate to binary phase coding and so these pictures square measure write in code with binary random part pictures by binary part XOR operation.

Mohammed Ali Bani Younes and Aman [19] introduce a block-based transformation rule supported the mix of image transformation and a well known encryption and coding rule referred to as Blowfish. The original image was divided into blocks, and victimization the transformation rule it absolutely was rearranged, and so the Blowfish rule is employed for encrypting the remodeled image their results showed that the correlation between image parts was considerably bated. Their results also show that increasing the amount of blocks by victimization smaller block sizes resulted in a very lower correlation and higher entropy.

S.S. Maniccam and N.G. Bourbakis have given a new rule that will 2 works: lossless compression and encoding of binary and gray-scale pictures. The compression and encoding schemes square measure supported SCAN patterns generated by the SCAN methodology. The SCAN is a formal language-based second spatial-accessing methodology generate a good vary of scanning methods or space filling curves.

REFERENCES

[1] Lini Abraham, Neenu Daniel ," Secure Image Encryption Algorithms: A Review", International Journal of Scientific & Technology Research volume 2, issue 4, April 2013, PP-186-189.

[2] Mohanraj Arumugam and Rabindra Kumar Singh, "Data Hiding and Extraction Using a Novel Reversible Method for Encrypted Image" IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 1, March, 2013, PP-1-5.

[3] Kim, H.J., Sachnev, V., Shi, Y.Q., Nam, J., Choo, H.G., 2008. A novel difference expansion transform for reversible data embedding. IEEE Transaction Information Forensics and Security 3 (3), 456–465.

[4] M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, "On compressing encrypted data," *IEEE Trans. Signal Process.*, vol. 52, no. 10, pp. 2992–3006, Oct. 2004.

[5] W. Liu, W. Zeng, L. Dong, and Q. Yao, "Efficient compression of encrypted grayscale images," *IEEE Trans. Image Process.*, vol. 19, no. 4, pp. 1097–1102, Apr. 2010.

[6] X. Zhang, "Separable reversible data hiding in encrypted image," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 826–832, Apr. 2012.

[7] X. Zhang, "Reversible data hiding in encrypted images," *IEEE Signal Process. Lett.*, vol. 18, no. 4, pp. 255–258, Apr. 2011.

[8] X. Zhang, "Lossy compression and iterative reconstruction for encrypted image," IEEE Trans. Inform. Forensics Security, vol. 6, no. 1,pp. 53–58, Feb. 2011.

[9] W. Puech" Image Encryption and Compression for Medical Image Security" PROCEEDING OF IEEE Image Processing Theory, Tools & Applications.

[10] W. Puech, M. Chaumont and O. Strauss "A Reversible Data Hiding Method for Encrypted Images" Author manuscript, published in "IS&T/SPIE Electronic Imaging 2008 - Security, Forensics, Steganography, and Watermarking of Multimedia Contents, San Jose, CA : United States".

[11] Kai-Hui Lee and Pei Ling Chiu "Digital Image Sharing by Diverse Image Media," IEEE Transaction On Information Forensics and Security,vol. 9,No. 1,January 2014.

[12] Shubhra Dixit, Deepak Kumar Jain, Ankita Saxena, "An Approach for Secret Sharing Using Randomised Visual Secret Sharing" 2014 Fourth International Conference on Communication Systems and Network Technologies.

[13] Hirdesh Kumar, Awadesh shrivastava,"A Secret Sharing Scheme for Secure Transmission for Color Image," 2014 International Conference On Issues and Challenges in Intelligent Computing Techniques(ICICT).

[14] Ms. Megha B. Goel, Mr. M. S. Chaudhari, Mrs. Shweta A. Gode," A Review on Data Hiding using Steganography & Visual Cryptography" 2014 IJEDR | Volume 2, Issue 1 | ISSN: 2321-9939.

[15] John Justin M, Manimurugan S,"A Survey on Various Encryption Techniques" International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-1, March 2012.

[16] WENJUN LU1, AVINASH L. VARNA2, (Member, IEEE), AND MIN WU3, (Fellow, IEEE)," Confidentiality-Preserving Image Search: A Comparative Study Between Homomorphic Encryption and Distance-Preserving Randomization", Digital Object Identifier 10.1109/ACCESS.2014.2307057 .

[17] Nitumoni Hazarika, Monjul Saikia," A Novel Partial Image Encryption using Chaotic Logistic Map", 2014 International Conference on Signal Processing and Integrated Networks (SPIN) 978-1-4799-2866-8/14/$31.00 ©2014 IEEE.

[18] Puja Devi Rana, Anita Singhrova, Suman Deswal," Design and Implementation of K-Split Segmentation Approach for Visual Cryptography", International Journal of Scientific and Research Publications, Volume 2, Issue 8, August 2012 1 ISSN 2250-3153.

[19] Abhinav Srivastava," A survey report on Different Techniques of Image Encryption" International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 6, June 2012).

BIOGRAPHIES

Ms. Snehal R.Awatade, has received her B.E. degree in Information Technology from IBSS College of Engineering, Amravati, India in 2013. Her area of research includes Cloud computing, Image processing, Database. Currently she is pursuing her M.E in Computer Engineering from Sipna COET Amravati India.

Dr. Avinash D.Gawande, has received his Ph.D. M.E in Computer Science and Engineering .His area of research includes Signal Processing, Information Storage and Data Recovery. Currently he is working as an Head of the Department of Computer Science and Engineering in Sipna COET Amravati, India.