Encryption and Data Hiding

Jeevan Bala
Lovely Professional University, Phagwara, Punjab, India,

Kamlesh Lakhwani
Lovely Professional University, Phagwara, Punjab, India.

***Abstract*—Encryption of data is done by every organization to provide security. It also provides confidentiality, integrity and authenticity to the data. Encryption along with data hiding techniques can provide maximum security to the data. The paper aims to put forward different algorithms for data hiding and data encryption, which in combination can ensure maximum security to data. This paper discuss several algorithm on data hiding and encryption having minimum data loss during its transmission over internet. Main focus of the paper is reversible data hiding in an image that is encrypted.**

Keywords – *component, encryption, reversible data hiding, image encryption, message, cover, image transformation, reversible color transformation.*

I. INTRODUCTION

In the world of internet, security of data floating over internet is a big question. When any data is sent over the network, we try to ensure its integrity and confidentiality [1]. When it comes to sending data in a secure manner, Cryptography comes in use; but Cryptography is one of the most challenging field to secure data transmission. Despite of different encryption algorithms being used in different organisations, the attackers are able to compromise valuable data of organisations on daily basis. An attacker is a unauthorized person/user who attempts to attack a communication or any organisation [2,3]. The aim is to protect those important data from the attackers [4,5,6].

There are two methodologies for protection of image content, 1. Encryption and 2. Data Hiding. Encryption is used to solve issues related to privacy, but the ciphertext generated after encryption algorithm is applied can get the attention of attacker. In data hiding we have a message and we embed this message into a cover, which can be an image, a video or an audio used to protect secret message. Data Hiding are of two types; Reversible and Non-reversible data hiding.

Earlier methods of Data Hiding are only suitable for smaller message size embedded into large size cover, e.g., image or audio. Moreover, embedding process can also cause permanent distortion to the cover. But in some cases distortion/degradation to the cover is not allowed such as medical or military imagery, law forensics etc. For that purpose we need a data hiding technique which cause no loss to cover. Reversible Data Hiding (RDH) technique, also known as lossless data hiding, can be efficiently used to recover the cover without any loss after the extraction of embedded message from it.

This technique has many useful application such as law enforcement, application in medical [7] to keep information of patient secret, in military its application occurs when we need secret information should be invisible from the eye of attacker and also we require lossless recovery of hidden secret information.

II. LITRATURE SURVEY

A. Secret Fragment Visible Mosaic Image to Information Hiding

Lai et al. [8] proposed a method for image transformation, which selected two similar images; one is target image and other is secret image then replacement is done on target image with respect to secret image. Replacement is done block wise means replace each block in target image by the similar block in secret image. This way encrypted image is formed. Method used for finding similar block is greedy search method. This is reversible

method but this method is suitable only when target image is similar to secret image. And also when encrypted then visual quality is poor.

B. Via Secret Fragment Visible Mosaic Image using Nearly Reversible Colour Transformations

Lee et al. [9] improved Lai et al.'s algorithm by transformation of secret image to target image which is selected randomly without the usage of database of any kind. Lee et al.'s modal included transformation of each block of large image into block of secret image by using reversible colour transformation method [10], then information required in restoration of secret image, such as block index, parameters, are added later to transformed blocks. Using Lee et al.'s method a secret image can be transformed into randomly selected target image. Lee et al.'s method does not support reversible transformation.

C. Using Public Key Cryptography

The Researcher [11] suggested a reversible, lossless information Hiding technique for Public-key-encryption images homomorphic and probabilistic cryptosystem's characteristics. By the usage of these schemes, reorganization or division of pixel is dodged and on pixels of cover directly encryption and decryption can be performed to lower or avoid the computational complexity and amount of data encrypted. Distortion on plain text domain can occur due to embedding of data on encrypted domain because of homomorphic properties, to recover the original content and for extraction of embedded data directly decryption of image is required. Some piece of information can be separated by recipient before unscrambling and the other piece of implanted information can be extricated and can recoup unique plain content and picture after decoding.

C. Via Key Modulation

Right now, to mystery encryption key isn't permitted. An amazing two class SVM classifier is planned toward the finish of decoder to recognize encoded picture patches from non-scrambled picture patches. This permits to translate the inserted message and unique picture together. This strategy is equipped for giving higher installing limit. Additionally, this technique is likewise skilled in remaking the installed message just as unique picture splendidly.

D. By Reversing Room before Encryption

Author [13] gave an alternate approachs for Reversible Data Hiding in scrambled picture. Right now, "room after encryption" isn't required which was done beforehand however right now room before encryption alongside conventional Reversible Data Hiding technique, consequently for the information hider it is anything but difficult to reversibly insert information into the picture. Utilizing this philosophies mistake free picture recuperations and information extraction can be accomplished. Right now first hard and fast rooms are made void by installing LSBs (Lowest Significant bits) of certain pixels into different pixels by utilizing conventional Reversible Data Hiding strategies and afterward encryption of picture is finished. This turning around room before encryption system separate information extraction from picture decoding and gives phenomenal execution.

E. Difference Expansion

Difference Expansion checks the digital image for redundancy to get high embedding capacity, and keep the very low amount of distortion. Jun Tian[13] embed both payload and original value after selecting an embedding area. In this method Reversible integer transform is applied. For gray scale evalued pair (8-bit) (x,y) x,y Є Z and 0<=x,y <=255,:

$$\text{(integer average) } I=(x+y)/2 \text{ and (difference) } h=x-y \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots(1)$$

for embedding bits b difference value h is used:

$$h'=2*h+b \quad \ldots\ldots\ldots\ldots..(2)$$

original values can be recovered using inverse integer transformation

$$x=1+(h+1)/2 \text{ and } y=1-(h/2) \quad \ldots\ldots\ldots\ldots..(3)$$

Picture is assembled into match of pixels and apply numbers transform. Difference esteem fall in four groups: expandable h=0, h=-1 (EZ), all expandable (EN), changeable (CN), non-changeable (NC). The subset of selected and non-selected distinct values are indicated as EN1 and EN2. Location outline is utilized to identify changeable contrast esteem ,1 shows chosen expandable distinction value. Location outline is at that point compressed to bit stream L. Collect the first LSB values of distinction values in EN2 and CN. 0Embed area outline L , original LSBs C and payload P. After all bits are implanted to B, converse numbers change is connected to obtain the inserted picture.

Category	Original Set	Original Value	Location map value	New Value	New Set
Changeable	EZ or EN1	h	1	2 * h + b	CH
	EN2 or CN	h	0	2 * |h/2| + b	
Non-changeable	NC	h	0	h	NC

Within the recovering prepare implanted bit stream B can be collected and hence can get the LSBs of all exchangeable contrast values. Area outline gives all the expandable contrast values. hence the original picture can be re-established. For contrast development based reversible information hiding, the implanted bit-stream mainly consisting two parts: one portion that passes on the secret message and the other portion that contains the binary (overflow) area outline and the header file. The primary portion is the payload whereas the second part is the auxiliary information bundle for blind detection. To extend implanting capacity, we have to be make the size of the second portion as little as conceivable. The compressibility of area outline should be expanded for distinctive sorts of images.

F. Modification of Histogram

In [14] Zhicheng Ni uses zero or maximum point of histogram of an image. The pixel gray scale values are somewhat adjusted to implant information into picture. In inserting process to begin with a histogram is created H(x). For designed histogram , discover the greatest vertex h(a) and least point zero h(b) .On the off chance that the least vertex h(b)>0, record the coordinate (u,v) for the pixels and the pixel gray scale esteem b as overhead bookkeeping information (referred overhead data for brief). At that point assign h(b)=0.Despite misfortune of simplification entire portion of the histogram with to correct by a unit, which implies that all the pixel gray scale values (satisfying) are included by 1. Check the image, when meet pixel (for which dark scale regard might be a), check the to-be-installed bit. In case the to-be embedded piece is "1", and the pixel dim scale regard is changed to a + 1 . On the off chance that the bit is "0", the pixel regard stays a. Deciphering is reasonable the rearrange plan. This strategy cannot be utilized for pictures with flat histogram.

For the improvement of the embedded capacity, A.S.AlFahoum [15] process another method is used. This strategy will be applied to the yield of Zhicheng's strategy .Yield from Zhicheng's strategy is isolated into similarly non- overlapping blocks. Contrast of histogram of each square is at that point extended to make additional inserting space. The bits are implanted into the space made after differentiate extending Pixel values in inserting ranges are modified by either including or subtracting one bit:

$$x''(i,j) = x'(u,v) - 1 \text{ if } x'(u,v) > \text{peak value} \quad \ldots\ldots(4)$$

$$x''(i,j) = x'(u,v) + 1 \text{ if } x'(u,v) < \text{peak value} \quad \ldots\ldots(5)$$

Another method based on storing and prediction is by V. Sachnev [16]. Information can be implanted by either cross implanting or dot implanting methods. Pixel esteem is anticipated based on encompassing pixels, then the forecast blunder is utilized for implanting information. The combination of histogram moving and expansion is utilized in this strategy. Forecast mistake between two limits is utilized for information implanting. The histogram move method embeds information with the edges. Cells are sorted in climbing arrange of the nearby fluctuation values. Cells with smaller fluctuation values are superior for information stowing away. In this way, the inserting handle begins from the cell with the smallest fluctuation esteem within the sorted push, and moves on to the following cells until the final bit of information is implanted.

H. Distributed Source Encoding

The main aim of this technique [17] is the improvement of reversible data hiding (RHD) for image which is encrypted by the use of Slepian-Wolf source encoding technique. This Slepiabn-Wolf technique is roused by DSC technique. After the first picture is scrambled by the substance proprietor with the utilization of stream figure, information hider pack the course of action of picked bits of the encoded picture to shape save space to fitting the mystery data. The proposed procedure is unmistakable because of the use of two particular keys. The shrouded data can be completely separated using the inserting key, and introductory picture can be duplicated with top notch using encryption key. In the event that the beneficiary have both the encryption and inserting keys, recipient can remove the mystery data and flawlessly recuperating the underlying picture. The proposed procedure accomplishes a high embeddings payload and extraordinary picture diversion quality and keeps up a vital good ways from the exercises of room-holding by sender.

I. BY Patch-Level Sparse Representations

The strategy called HC_SRDHEI is proposed in [18], that procures the advantages of RRBE, and along these lines noticeability properties of RDH techniques in scrambled pictures for the better association between among pixels, we propose consider the fix level insufficient portrayal when concealing the mystery data. Contrasted with best in class decisions, the room cleared for data covering up. The data hider essentially gets the pixel substitution to substitute the open stay with additional mystery data. The data extraction and spread picture recovery are recognizable, and are liberated from any misstep. Test comes to fruition on three informational indexes creates the impression that the proposed procedure has ordinary MER an arrive at 1.7 occasions as tremendous as the past best elective technique gives. The execution examination recommends that proposed technique incorporates a particularly extraordinary potential for reasonable applications.

III. PROPOSED WORK

In this paper, we proposed a research including two aspects in the strategy:

• Alter the change to be reversible.

• Progress the nature of disguise picture by setting the more diminutive tile size.

The system designed in the paper redesigns Lee et al's. system [19]. The designed framework, do change for channel R, G, B of a concealing picture self-rulingly, so we sensible take the change on dull pictures (one channel) as a portrayal. In proposed strategy the puzzle picture and the target picture are restricted into N non-covering pieces with a comparative check, which are called tiles. The secret tiles are organized into a course of action B I and the target tiles are masterminded into another progression Ti as demonstrated by the SD of the pixels in each tile. Likewise, after that the ith riddle tile is changed to the ith target tile with the reversible picture change.

Work designed is distributer in three parts:--

- Content Owner,
- Receiver
- Data Hider

IV. CONCLUSION

Conventional procedures of reversible information covering up into scrambled picture confronted a couple of limitation, that are inadequate for assurance of picture substance, it can't make sure about the data, lesser concealing limit and complex calculations, lucidity of the picture will be down and out, data pressure isn't proficient, some issue inside the interpreting portion. Underneath the solicitations to beat such sort of disadvantages proposes a novel arrangement of Information Stowing ceaselessly in Encrypted Image by the RIT, which can change a mystery picture to a randomly picked target picture for getting a mixed picture that is used as the encryption of mystery picture with incredible visual quality, and mystery picture can be restored with no disaster.

REFERENCES

[1] Achuthshankar, A., & Achuthshankar, A. (2015, January). A novel symmetric cryptography algorithm for fast and secure encryption. In 2015 IEEE 9th International Conference on Intelligent Systems and Control (ISCO) (pp. 1-6). IEEE.

[2] Kocheta, M., Sujatha, N., Sivakanya, K., Srikanth, R., Shetty, S., & Mohan, P. A. (2013, December). A review of some recent stream ciphers. In 2013 International conference on Circuits, Controls and Communications (CCUBE) (pp. 1-6). IEEE.

[3] Abumuala, M., Khalifa, O., & Hashim, A. H. A. (2010, May). A new method for generating cryptographically strong sequences of pseudo random bits for stream cipher. In International Conference on Computer and Communication Engineering (ICCCE'10) (pp. 1-4). IEEE.

[4] Ding, L., Jin, C., Guan, J., & Wang, Q. (2014). Cryptanalysis of lightweight WG-8 stream cipher. IEEE transactions on information forensics and security, 9(4), 645-652.

[5] Lamba, C. S. (2010, February). Design and analysis of stream cipher for network security. In 2010 Second International Conference on Communication Software and Networks (pp. 562-567). IEEE.

[6] Stallings, W. (2006). Cryptography and network security, 4/E. Pearson Education India.

[7] Bao, F., Deng, R. H., Ooi, B. C., & Yang, Y. (2005). Tailored reversible watermarking schemes for authentication of electronic clinical atlas. IEEE Transactions on information technology in biomedicine, 9(4), 554-563.

[8] Lai, I. J., & Tsai, W. H. (2011). Secret-fragment-visible mosaic image–a new computer art and its application to information hiding. IEEE transactions on information forensics and security, 6(3), 936-945.

[9] Lee, Y. L., & Tsai, W. H. (2013). A new secure image transmission technique via secret-fragment-visible mosaic images by nearly reversible color transformations. IEEE Transactions on circuits and systems for video technology, 24(4), 695-703.

[10] Reinhard, E., Adhikhmin, M., Gooch, B., & Shirley, P. (2001). Color transfer between images. IEEE Computer graphics and applications, 21(5), 34-41.

[11] Bartwal, M., & Bharti, R. (2017). Lossless and Reversible Data Hiding in Encrypted Images With Public Key Cryptography. Annals of Computer Science and Information Systems, 10, 127-134.

[12] Zhou, J., Sun, W., Dong, L., Liu, X., Au, O. C., & Tang, Y. Y. (2015). Secure reversible image data hiding over encrypted domain via key modulation. IEEE transactions on circuits and systems for video technology, 26(3), 441-452.

[13] Tian, J. (2003). Reversible data embedding using a difference expansion. IEEE transactions on circuits and systems for video technology, 13(8), 890-896.

[14] Ni, Z., Shi, Y. Q., Ansari, N., & Su, W. (2006). Reversible data hiding. IEEE Transactions on circuits and systems for video technology, 16(3), 354-362.

[15] Al-Fahoum, A. S., & Yaser, M. (2013). Reversible data hiding using contrast enhancement approach. International Journal of Image Processing (IJIP), 7(3), 248.

[16] Sachnev, V., Kim, H. J., Nam, J., Suresh, S., & Shi, Y. Q. (2009). Reversible watermarking algorithm using sorting and prediction. IEEE Transactions on Circuits and Systems for Video Technology, 19(7), 989-999.

[17] Qian, Z., & Zhang, X. (2015). Reversible data hiding in encrypted images with distributed source encoding. IEEE Transactions on Circuits and Systems for Video Technology, 26(4), 636-646.

[18] Cao, X., Du, L., Wei, X., Meng, D., & Guo, X. (2015). High capacity reversible data hiding in encrypted images by patch-level sparse representation. IEEE transactions on cybernetics, 46(5), 1132-1143.

[19] Singhavi, D. G., & Chatur, P. N. (2015, March). A new method for creation of secret-fragment-visible-mosaic image for secure communication. In 2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS) (pp. 1-5). IEEE.