Separable and Error-Free Reversible Data Hiding in Encrypted Image Based on Two-Layer Pixel Errors

[1]Mr.Satish Manje, [2]Mr.Saurabh Fule, [3]Mr.Tejas Kamble, [4]Mr.Rickain Solanki
[1]Asst.Professor, [2,3,4]UG Student,[1,2,3,4]Computer Engg. Dept. Shivajirao S. Jondhle College of Engineering & Technology, Asangaon, Maharashtra, India.
[1]satishmanje93@gmail.com,[2]fsaurabh666@gmail.com,[3]tejaspkamble5@gmail.com,
[4]rickainsolanki55@gmail.com

Abstract - Data is very crucial part in human's life. One can get easy access to data of unknown person while communication between two persons in that case any third person can get that data by some techniques. To avoid such things, Data in Image Encryption has been developed. It plays significant role in field of cryptography. Data is hidden behind image for more secure transmission of data. Reversible data hiding is important topic of data hiding. This paper proposes a novel "separable and error-free reversible data hiding in encrypted image based on two-layer pixel errors". Specifically, proposed scheme divides original image into series of non-overlapped block. Closed Hilbert curve is used for scanning each block to obtain one-dimensional pixel sequence. Pixels of sequence are encrypted with key transmission. During data hiding, each non-overlapped block of encrypted image is scanned in closed Hilbert order to generate one-dimensional encrypted pixel sequence.

Keywords – Error, Data Hiding, Encrypted, Pixel.

I. INTRODUCTION

There are lot of troubles caused by development of digital era. These may range from nuisances situations that are catastrophic to life, career and financial security that can literally harm human's life dangerously. Main threats are Identity thefts (Hacker steals identity of Victim), Personal information leaks (personal information can be leaked to defame that person), Bank Frauds, Website Security Breaches, Internet Trolls most vulnerable thing that can happen to humans is when they are sharing their data across the digital medium. The data can be a document file, excel file, image or a video. This can contains crucial data of person. In organization if manager tries to send file to employee and while transferring file any third person tries to hack and manipulates file in such manner integrity of file is lost and manipulated file is reached to employee it will tedious for both of them and attacker will get profit in terms of money. To prevent this there is concept known as Steganography.

II. AIMS AND OBJECTIVE

a) Aim

Aim of making this system to implement and improve performance of Advanced Image Encryption Data Hiding process to provide secure, reliable and loss less data transmission over internet. Data hiding is efficient technique which aims is to provide security to data which is transferred from sender and receiver. Different Techniques should be used to protect confidential image data from unauthorized access as each type of data has its own features.

b) Objective

Without any loss of original data and original image quality. Data is transferred and securely encrypted in image. It can be used in many applications such as schools, colleges, and government offices, military by using encryption techniques. Integrity of data and session is maintained while sharing of data. Objective of study is to develop System which can provide data hiding technique and image Encryption in which data can be retrieved.

III. LITERATURE SURVEY

1] Tamilselvi R, Ravindran G. Image encryption using pseudo random bit generator based on logistic maps with radon transform, Vol (8-11). Indian Journal of Science and Technology June-10-2015.

Algorithm using logistics map and Radon transform. It aims is to finding an optimum transformation technique that gives better encryption in terms of encryption quality and entropy. Methods/Analysis: A Pseudo Random Bit Generator (PRBG) is used which outputs sequence of statistically independent and unbiased binary digits. According to what data is being encrypted the priority of

 DOI : 10.35291/2454-9150.2020.0224

the key is set. Maximum encryption occurs when angle of rotation is 135. Similarly, the results of entropy value indicate that there is higher encryption of 80% for 135 degree of rotation

2] Smitha, M., Jayanthi, V. E., & Merlin, A. (2013). Image encryption using separable reversible data hiding scheme. 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT). July-4 2013, Tiruchengode, India.

Image Encryption has significant role in field of cryptography. A New Encryption scheme is introduced to protect image from unauthorized access, in this scheme two separate keys are used for image encryption and data hiding with high degree of security. Additional data. Run-Length Coding (RLC) and Haar Wavelet compression technique. It includes low significant bit as well as maximum significant bit for encrypting and decrypting data and image for accuracy. Compression of data sometimes leads to ambiguous data and not so accurate. In this scheme user can extract an image, data and both image and data based on the key used.

3] Zhang L, Zhang D, Mou X, Zhang L. FSIM: A Feature Similarity Index for Image Quality Assessment. Vol (20) IEEE January-31-2011.

Image quality assessment (IQA) aims to use computational models to measure the image quality consistently with subjective evaluations. In this paper, a novel feature similarity (FSIM) index for full reference IQA is proposed based on fact that human visual system (HVS) understands an image mainly according to its low-level features.

4] Celik MU, Sharma G, Tekalp AM, Saber E LOSSLESS GENERALIZED-LSB DATA EMBEDDING. Vol 14 IEEE Transactions on Image Processing. February-2-2005.

Exact recovery of original host signal upon extraction of embedded information. A generalization of well-known least significant bit (LSB) modification is proposed as data-embedding method, which introduces additional operating points on capacity-distortion.

IV. EXISTING SYSTEM

In existing system, JPEG bit stream method is used to hide data in encrypted image. The scheme is defined the principle content of original image while preserving the bit stream structure. In JPEG bit stream technique secret bits are encoded with error correction codes and then embedded into JPEG bit stream. On receiving side, neighboring blocks are used to extract the secret bits and restore the original bit stream.

Drawbacks of Existing system:

It works only with JPEG (Joint Photographic Experts Group) image file format. The cover image should be in JPEG format. There is a limitation on data size to be embedded on the cover image. There are chances of losing the data.

V. COMPARTIVE STUDY

SR NO.	PAPER TITLE	AUTHOR NAME	METHOD	ADVANTAGE	DISADVANTAGE
1.	Image encryption using pseudo random bit generator based on logistic maps with radon transform	Tamilselvi R, Ravindran G.	Random sets algorithm are used according to the priority of the data if the data is crucial then random algorithm is used if not then single algorithm is used.	Combination of more than one cryptographic algorithm. Most Secured. Not easy to guess	Time Consuming
2.	Image encryption using separable reversible data hiding scheme	Smitha, M., Jayanthi, V. E., &Merlin (ICCCNT).	Lowest significant and Maximum significant bit & Reversible scheme.	More secure Uses LSB and MSB concept to compress and decompress.	Difficult to understand, complex
3.	FSIM: A Feature Similarity Index for Image Quality Assessment.	Zhang L, Zhang D, Mou X, Zhang L.	Pixel Matrix concept is used Gradient Magnitude. Usually deals with graphical objects.	Mainly focuses on the quality of the image by using Image Quality Assessment metrics, very robust.	Image quality differs from original one.
4	Lossless Generalized-LSB DATA Embeddi-ng	Celik MU, Sharma G, Tekalp AM, Saber E.	Recovering the embedded points.	enables the exact recovery of the original host signal upon extraction of the embedded information	Little Bit time Consuming

VI. PROBLEM STATEMENT

In normal communication transferring data from one place to another there is chance of getting data to be hacked in between sender and receiver by attacker mainly aiming to destroy integrity. Outdated encryption and decryption techniques. Complexity is more in techniques such that data can be encrypted.

VII. PROPOSED SYSTEM

Error less Reversible Data Hiding

A content owner encrypts original uncompressed image using encryption key to produce encrypted image. Data

 DOI : 10.35291/2454-9150.2020.0224

hider embeds secret data into encrypted image to obtain marked encrypted image according to data-hiding key. Then, with marked encrypted image, receiver extracts secret data using data-hiding key. A directly decrypted image with good quality can be obtained by decryption. If receiver has encryption key.

A. IMAGE ENCRYPTION

Image encryption consists of two components: block permutation and transmission encryption. Two closed Hilbert orders are constructed as depicted in figure below for scanning pixels of permutated blocks. Since Hilbert orders are closed, all pixels can be traced beginning with any pixel in one block.

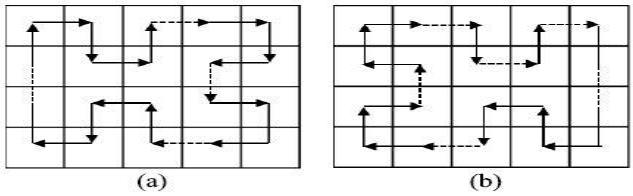

Fig1. Closed Hilbert's curve

Ability to get pixel original image create a strong Encryption image such that it cannot be hacked easily. Closed Hilbert curved is used to generate empty pixel in image which are used in combinations with other pixels for encryption.

B. DATA HIDING IN ENCRYPTED IMAGE

Since relative positions between two adjacent original pixels in each permutated block are preserved during encryption as described in Section II A.

C. DATA EXTRACTION AND IMAGE RECOVERY

At receiver side, different keys held by receiver determine different operations he or she can perform, respectively.

VIII. ALGORITHM

General idea of working proposed system algorithm is given as follow:

STEP 1: START
STEP 2: ENCRYPTION
Input: Image File
Output: Encrypted Image File
STEP 2.1: Generation of 8-bit binary Encryption key(K1)
STEP 2.2: Perform EX-OR operation on pixels and encryption key(K1)
STEP 3: DATA HIDING
STEP 3.1: Perform LSB compression on encrypted pixels
STEP 3.2: Generation of data hiding key (K2)
STEP 3.3: Select random EN pixels
STEP 3.4: EN pixels hide using data hiding key (K2)
STEP 4: DATA EMBEDDING
STEP 4.1: Generation of additional data
STEP 4.2: Additional data and EN Pixels embedded
STEP 5: DECRYPTION:
Input: Encrypted Image, KEY
Output: Original Image, DATA
STEP 5.1: Enter KEY
STEP 5.2: If Sender's KEY == Receiver's key
STEP 5.3: Return Original Image and DATA
STEP 5.4: Else go to STEP 5.1
STEP 6: END

IX. MATHEMATICAL MODULE

1] IMAGE ENCRYPTION:-

Image encryption consists of two components: Block Permutation and Transmission encryption.

$$Ci+1 = rci(1 - ci), \quad 0 \le r \le 4, ci \in (0, 1) \qquad (1)$$

2] DATA HIDING IN ENCRYPTED IMAGE:-

The histogram of two-layer adjacent encrypted pixel errors is accommodated for data hiding. Since data hiding is achieved by histogram shifting in paper, overflow or underflow may occur as most reversible data hiding based on histogram shifting.

$$EX2 = \begin{Bmatrix} EX1 = \{EB1, EB2, \ldots EBr\text{-}1\} \\ \{EBr, EBr+1, \ldots EBN\} \end{Bmatrix} \qquad (2)$$

3] HISTOGRAM GENERATION OF TWO LAYER ENCRYPTED PIXEL ERRORS:-

In this part, keys *Kp*, *Kb* and *Kt* are unknown to data hider. Data hider selects

Closed Hilbert order for **EB** according to logistic map and key *c*0 described in section A.

4] DATA EMBEDDING:- After obtaining two layer encrypted pixel errors histogram, secret data can be embedded into encrypted image by histogram shifting. To embed data in image for encrypting it.

$$d1(i)' = \begin{cases} d1(i), & if\ 1<=i<=2 \\ d1(i-1) - d2(i)', & if\ 3<=i<=m \end{cases} \qquad (4)$$

5] DATA EXTRACTION AND IMAGE RECOVERY:-

At receiver side, different keys held by receiver determine different operations he or she can perform, respectively.

$$di' = \begin{cases} (e'i-k) \bmod 256 & if\ i=1 \\ (e'i-e'i-1) \bmod 256 & if\ 2<=i<=m \end{cases} \qquad (5)$$

 DOI : 10.35291/2454-9150.2020.0224

X. SYSTEM ARCHITECTURE

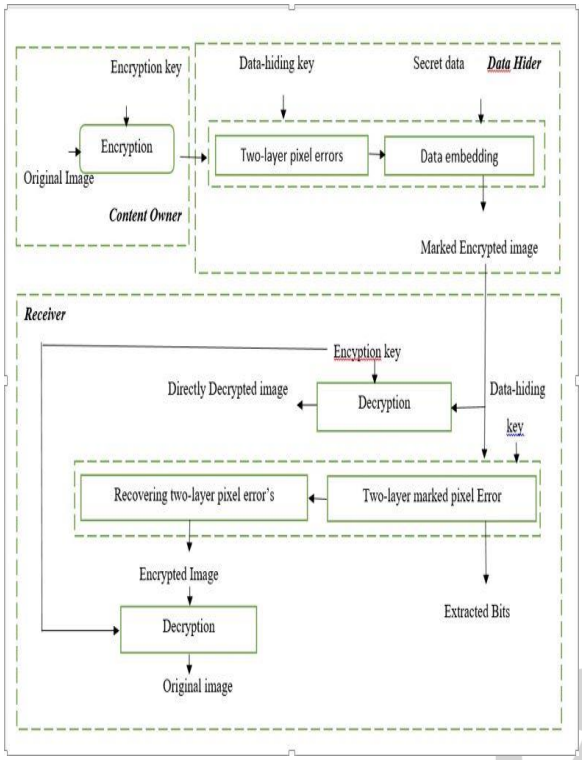

Fig.2: System Architecture

Description:

Admin is super or root user who has right to control all operations which performed in system. In this module, Admin can login by using valid Username & Password. Only admin has authority to access user details. After successful login, admin can do various operations.

In this module, new user can register by itself in register section by filling user registration form. In user registration form, user has to fill following details in order to registered i.e. Login ID, password, email id and address. User can login into system with registered username and password .

XII. DESIGN DETAILS

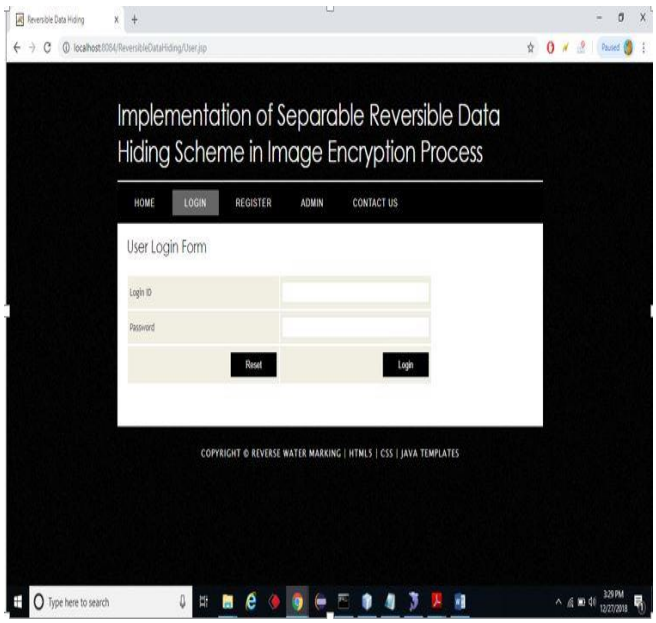

Fig3. Login Page.

XI. ADVANTAGES

1. Accurate data Quality is properly maintained
2. Mainly focuses on the quality of the image by using Image Quality Assessment metrics, very robust.
3. No loss of data. Improves the efficiency
4. It uses cryptographic concepts to encrypt the data behind and image.
5. More secure.

XIII. CONCLUSION

Thus, we have tried to implement the paper "Chunqiang Yu, Xianquan Zhang, Zhenjun Tang, and Xiaojun Xie.", "*Separable and Errorless Reversible Data Hiding scheme in encrypted image using two layer pixel error.*" IEEE 2018. A novel separable reversible data hiding scheme is implemented for image encryption. An input image is encrypted by the content owner using an encryption key. Data hiding key compresses the least significant bits of the encrypted image to create space to embed a data. Image encryption key is used to retrieve the image and data hiding key for data extraction. Image encryption and data hiding keys can be used for simultaneous extraction of the original content by exploiting the spatial correlation in natural image. Simulation results obtained is similar to the natural content. In future, various other compression techniques can be employed for further studies.

REFERENCE

[1] Kodituwakku SR, Amarasinghe US. Comparison of Lossless Data Compression Algorithms for Text Data. Indian Journal of Computer Science and Engineering 2010.

[2] Lai YK, Kuo JCC. A Haar Wavelet Approach to Compressed Image Quality Measurement. Journal of Visual Communication and Image Representation 1999.

[3] Alam FI, Khanam Bappee F, Khondker FUA. An Investigation into Encrypted Message Hiding hrough Images Using LSB. International Journal of Engineering Science and Technology (IJEST) 2011.

[4] Bhattacharyya D, Roy A, Roy P, Kim TH. Receiver Compatible Data Hiding in Color Image. International Journal of Advanced Science and Technology 2009.

[5] Puech W, Chaumont M, Strauss O. A Reversible Data Hiding Method for Encrypted Images. San Jose, CA, USA: SPIE, IS&T'08: SPIE Electronic Imaging, Security, Forensics, Steganography, and Watermarking of Multimedia Contents 2008.

 DOI : 10.35291/2454-9150.2020.0224