Hybrid Approach for Data & Image Encryption using LSB, RDH and AES Algorithm

Ms. V. Sivaranjani[1]
PG Scholar, Department of CSE,
Sri Vidya College of Engineering and Technology,
Virudhunagar dist, India,

Ms. V. Bhuvaneshwari[2]
Assistant Professor, Department of CSE,
Sri Vidya College of Engineering and Technology,
Virudhunagar dist, India,

Abstract— **Hacking is the most crucial problem during transmission time. Unauthorized should hack a different persons personal data or any organization secrets were hacked during interchange the facts. In this paper, we proposed the archive data and image dispatch. It mainly focused on the prudence. Advanced Encryption standard (AES) is used to increase the security in images. Hybrid of Least Significant Bit (LSB) and Reversible Data Hiding (RDH) technique which can be used for data hiding and data embedding in encrypted images. It mainly focused on medical and military purposes. eg: It is a war between two countries A and B, the chief of the country A can send their attack in step by step process. They can send in before the battle as the time limitation is little. suppose it was hacked by the other country person B definitely they can protect them self and they can get clear idea to face the circumstances. Making a good plan there is a chance for failure for A. So, confidentiality is important in the field.**

Keywords— LSB, AES, Embedding, Encryption, RDH, Decryption

I. INTRODUCTION

A novel approach used here is to hide the data a during transmission using multiple algorithms. Lossless crush is used here after data loss. Using Reverse Room Before Encryption is used to enlarge the image while encryption to store more information. Get two screws for two divergent movement. Kede Ma, Weiming Zhang, Xianfeng Zhao, Nenghai Yu, and Fenghua Li[1], [2]Using data hiding and image encryption under separate key. Allocate separate space for data. Using DWT split image in to four parts, namely LL, HL, LH and HH. LL contains MSB of original image. Data hiding in LSB avoid data loss. To enrich security high in LL contains original image. Arnold scrambling used in upper part HL, LH and HH to hide the data. XOR operation used here. Di Xiao and Shoukuo Chen. [3]To decrease the transmission time compression is necessary. Confidential transmission and video surveillance we enrich the image security. AES algorithm used for hiding the content. AES algorithm which contain iterative rounds. AES algorithm support several cipher modes of operation such as ECB (Electronic Code BooK), CBC (Cipher Block chaining), OFB(Output Feedback), CFB(Cipher Feedback) and CTR(Counter). W.Puech, M.Chaumont and O.Strauss.

[4] Insecure channel during transmission compress and encrypt the original data. Encryption increase the efficiency and then secrecy. Reversal is possible during the decryption of the data source use the secret key to encrypt the data and then compressed. Decompression occur use the secret key. To Review the problem of the Distributed Source Coding(DSR). They can provide scenarios for both lossy and lossless compression. The most stronger notation is Shannon-sense perfect secrecy. Siva Theja Maguluri.

[5]In image encryption process the histogram shifting is used to estimating errors of some pixels and emitted space used for data hiding. Data embedding in encrypted image. Two different schemes, extraction before decryption and decryption before extraction, are raised to cope with different applications. without encryption key, the unauthorized person is tedious to get details of original images. weiming Zhang, KedeMa, Nenghaiyu.

[6] Need for confidentiality under the situation. They can mingle two techniques to embed the data in existing system. In proposed system, three LSB encryption techniques utilized. It mainly focused on CAI. This system not only enhances the security of data but also support effective ways for protecting data. To enhance the security of data and then to compare three steganographic techniques, this system, data is encrypted with RC4 encryption algorithm. Wai Wai Zin, Than Naing Soe. [7]To improve the capacity of the hidden secret data and provide an stego image quality, a novel method based on image contrast is presented. A group of 2×2 blocks of non-overlapping spatially adjacent pixels is selected for embedding the secret message. The modulo 4 arithmetic operation is applied to embed a pair of binary bits is modified. Each secret message is also encrypted by RSA encryption algorithm. K.Pramitha, Dr.L.PadmaSuresh, K.L.Shunmuganathan.

[8]In-corruption is a method which can be subdivided a single block. Each block contains secret bit. The secret block which can be used for hidden the data. To find a host pixel for each block. To insert a secret bit for each block, the image quality improved. Kuang Tsan Lin. [9]Cryptography involves converting a message text into an encrypted format. steganography embeds message into a cover

media and hides its endurance. Both these approach provide some security for sensitive data and are vulnerable to intruder attacks. An advanced system of encrypting data that combines the features of cryptography & steganography methods. This system will be more secure. Piyush Marwaha, Paresh Marwaha.

[10] RDH extraction focused on confidentiality without data loss occur. Real reversibility is possible. Data extraction and image recovery are free of error. Both image and data have equal importance. No distortion of the original cover is allowed. Besteena K J, Philumon Joseph. [11]It proposes a novel RDH scheme for in-corruption image. After encrypting the original content of an uncompressed image by stream cipher, the additional data can be embedded in to the image by modified small proportion of in-corruption facts. Xinpeng Zhang.

[12] security and confidentiality needed for the sensitive data, Unreliable and unsecured network communication. RDH technique in VRBE method paid way to overcome certain defects. AES algorithm used for encrypted image and data. Tackling the problem of data loss while communication network. original image split in to two parts A and B one for data hiding and embedding and another for image encryption based on LSB significant. Deepthi.c. [13] compression technique is used to minimize the data size. Lossless technique is used for encrypt the data. Reduced complexity they used turbocodes. M.Johnson, P.Ishwar, V.M.Prabhakaran, D.Schonberg and K.Ramchandran.

[14]watermarking is a technique to protect from hackers while transmit the data. Robust and fragile watermarking is two types. Fragile watermarking is used without data loss and more authentication is possible. Arithmetic coding is used for the data hiding technique. Jun Tian. [15] Protect the data from the stranger's, they used hiding technique. Hiding mainly focused on histogram shifting, not only consider nearby value, It only based on global search of data. Xiang Wang, Qingqi Pei, Xinbo Gao and Hui Li. [16]original content, we consider matrix format. Choose least significant bit to change the content to be hide. Using compression technique reduced both time and cost complexity. Max capacity is less than 1. M.U.Celik, G.Sharma, A.M.Tekalp and E.Saber.

[17]Encrypt image and data under multiple secret key. The user get one key they can get only the specified one. SHA-1 algorithm is used for the authentication purposes. They can apply this process under the spatial domain. C.Anuradha, S.Lavanya. [18]Hide the content based on sequential approach using cs to reduced cost. Liangjun Wang, Xiaolin Wu, Fellow and Guangming Shi.

II. RELATED WORKS

A novel method applied to hide the content ensure more security. Real reversibility is possible. It contains 10 times speed larger than older one. Image and data recovery using different Keys. Error free & Increase confidentiality. eg: Data stored in the cloud storage. The user has only key for data he can get only data. The user only authorized for image he can get only the image.[1] There are generally two types of compression. They are lossy and lossless compression.

Lossy Compression:

It can loss some data during retrieval time.

Lossless Compression:

It cannot occur data missing retrieve the related images(original image)[5]. Stegneography: Security maintains of data. P to C and C to P conversion. Widely used in banking purposes in real world[6]. Spatial Domain: It means changing an image representing an object in space to enhance the image for a given application.RSA which means Rivest Shamir Adleman[7].

In secrecy maintenance we use public and private keys. Given input image. we consider image in matrix format m*n. In image processing RGB color contain high priority. so consider RGB color is given input we cannot allocate for data, it will be allowed for only image. Using filter the another color's in image is only for embedded the data. In encryption we split space of given input in to two parts LSB and MSB. Hiding based on binary value changing [6][2][12].HS is mainly used for collection of statically application of images. The images in the form of discrete format. It can be widely used in real time application in census report survive in the yearly once. Their current status of their organization. To improve their security[15].Cryptography is a technique used for protect the data from unknown person. It maintains secrecy between the two person user and sender. During data transmission period the third party cannot know without the key is a good trend. A key cannot easily hack by someone. It mainly used in military field.

[9]First to select the host part and then sequential difference to find the values of each pixel to select the best part for data and image, without data they can retain the originality which is possible

III. PROPOSED WORK

we proposed three keys for data and image to improve the security throughout the world. Hiding the image and data. AES algorithm used for encryption in image. Data encryption and data embedding. we use hybrid of LSB and RDH algorithm.

Need for encryption

Protect the user sensitive data from the hackers. They used secret key to protect their data. They can increase confidentiality.

Need for Decryption

Receiver decrypts the data using authorized key only. The key contains two types.

Public key and
Private key

Public Key

Sender and receiver using a single key for data encryption and decryption process.

Private Key

They used two different Keys for encryption and decryption.

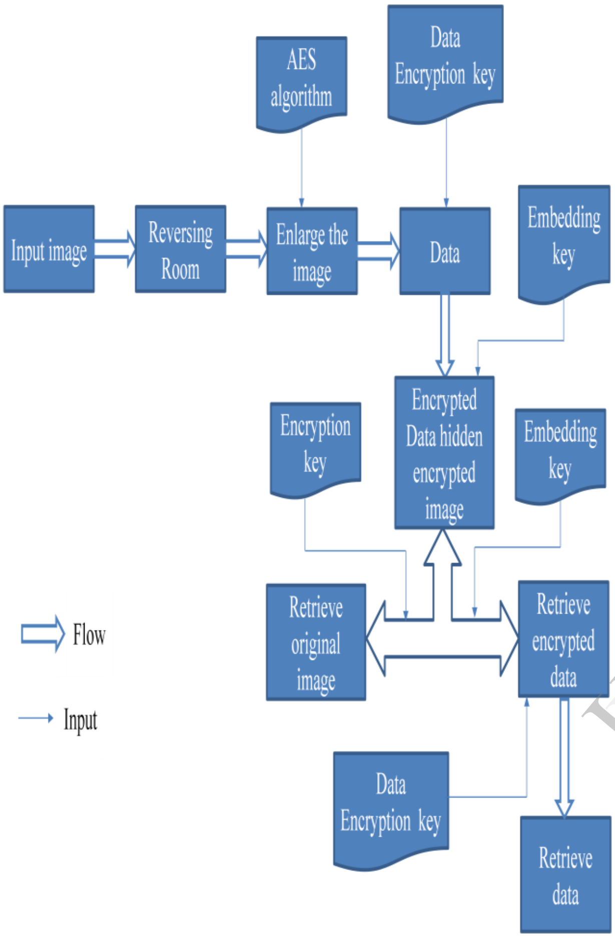


Fig 1: ARCHITECTURE

AES Algorithm

AES algorithm is a block cipher of length 256 - bit key. AES algorithm used for encryption and decryption of images. It contains 4 steps to encrypt images.

Byte Substitution
Shift Rows
Mix Columns and
Add Round Key

Byte Substitution

S-box to perform byte by byte substitution method. The values are fixed. Decryption contains inverse of the table.

For eg

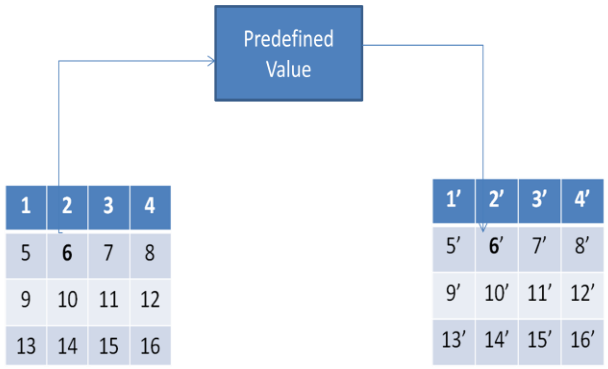


Fig 2: Byte Substitution

Using s-box table to find the inverse for given value.

Shift Rows

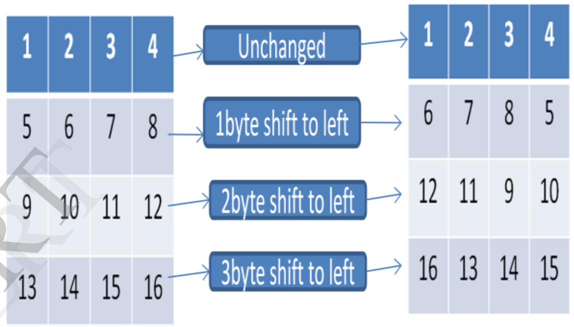


Fig 3: Shift Rows

It can contains the circular rotate of each rows. First row cannot modify. second row one circular shift to left. Third row 2 circular shift to right. Fourth row three circular shift to left.

Mix Column

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Fig 4: Before Mix Column

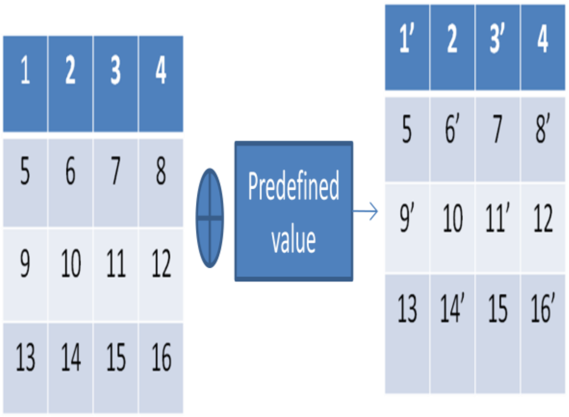
Above matrix will be substituted using a predefined matrix value.(2 3 1 1) by (1 5 913),(1 2 3 1) by(2 6 10 14),(1 1 2 3) by (3 7 11 15) and (3 1 1 2) by (4 8 12 16). (2 3 1 1) multiply (1 5 9 13) then we get (2 15 9 13).Then matrix formation will occur.

2	2	3	4
15	6	7	8
9	10	11	12
13	14	15	16

Fig 5: After Mix Column

Add Round Key

It contains XOR operation with key in each block generated a value with high efficient and secure one. Inverse of decryption identical. since XOR operation with own inverse which create reversed keys. Designed to be simple as possible.



1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

1′	2	3′	4
5	6′	7	8′
9′	10	11′	12
13	14′	15	16′

Fig 6: Add Round Key

LSB Algorithm

Step 1: Select a original image of size M*N as an input.

Step 2: The data to be hide based on RGB component.

Step 3: Select a best pixel from the original image to hide the sensitive information.

Step 4: Using a filter is applied to split the bit into two parts.

Step 5: One is LSB and MSB.

Step 6: Leaving MSB to encrypt the data in LSB by bit replacement.

Step 7:Real reversibility is possible.

eg:

Original image in matrix format

10010000	10010011	10011010
10010001	10010101	10010000
10010101	10010000	10011000

Leaving MSB

10010000	10010011	10011010
10010001	10010101	10010000
10010101	10010000	10011000

Hide LSB

10010000	10010010	10011000
10010001	10010100	10010000
10010100	10010000	10011000

CONCLUSION

Increasing privacy from the hackers, we use data and image encryption. Use AES algorithm to hide the original image. Using LSB approach without data loss and achieve excellent result. Two different keys used in this process to increase the confidentiality.

FUTURE WORK

To increase the keys to improve the confidentiality in that process. RDH technique used in that process for data extraction.

REFERENCES

1. Kede Ma, Weimming Zhang, Xianfeng Zhao, Nenghai Yu and Fenghua Li, "Reversible Data hiding in encrypted images by Reserving Room Before Encryption," IEEE Transactions on Information Forensics and security, Vol.8,No.3, March 2013.
2. Di Xiao and Shukuo Chen, "Separable data hiding in encrypted image based on compressive sensing," Electronics Letters Vol.50,No.8, April 2014.
3. W.Puech, M.Chaumont and O.Strauss, "A Reversible Data hiding method for encrypted images," Lirmm Laboratory, UMR CNRS 5506, University of Montpellier ||, France.
4. Siva Theja Maguluri, "Compressing encrypted Data," ECE 559RB Cryptography May 2009.
5. Weiming Zhang, Kede Ma, Nenghai Yu, "Reversibility improved data hiding in encrypted images," school of information science and technology, University of science and technology of china.
6. Wai Wai Zin and Than Naing Soe, "Implementation and analysis of three steganographic approaches," ICCRD 2011, 3rd conference on Volume-2
7. K.Pramitha, Dr.L.Padma Suresh, K.L.Shunmuganathan, "Image Steganography using mod-4 embedding algorithm based on image contrast," proceedings of 2011, International Conference on Signal Processing, Communication, computing and networking technologies (ICSCCN 2011)
8. Kuang Tsan Lin, "Data encrypting in a binary image base on modified data hiding method," proceeding IIH-MSP '11 Proceedings of the 2011 seventh international conference on intelligent information hiding and multimedia signal processing.

9. Piyush Marwaha and Paresh Marwaha, "Visual cryptographic steganography in images," Proceedings of international conference on computing and networking technologies, p.p.1-6, 2010
10. Besteena K J & Philumon joseph, "Secure reversible data hiding in encrypted images by reserving space in advance," International journal of research, Volume-1, Issue-6,july 2014
11. Xinpeng Zhang, "Reversible data hiding in encrypted image," IEEE signal processing letters, 18(4), pp.255-258, 2011
12. Deepthi.C, "Highly secured reversible data hiding in AES encrypted images by reserving room before encryption with authentication," IJCAT International Journal of computing and technology,Volume1,Issue4,May 2014.
13. 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.
14. Jun Tian, "Reversible Data embedding using a difference expansion," IEEE Transactions on circuits and systems for video technology, Vol.13,No.8,August 2003.
15. Xiang Wang, Qingqi Pei, Xinbo Gao and Hui Li, "Reversible data hiding by combining local and global search," International journal of innovative computing, information and control ICIC International Volume.9, No.2,Feb 2013
16. M.U.Celik, G.Sharma, A.M.Tekalp & E.Saber, "Lossless generalized - LSB data embedding," IEEE Trans.Image Process., Vol.14, no.2, pp. 253-266, Feb 2005.
17. C.Anuradha & S.Lavanya, "Secure and authenticated reversible data hiding in encrypted image", International journal of advanced research in computer science and software engineering, Volume3, Issue4, April 2003.
18. William Stallings, "Cryptography and Network security". Third edition.