American Journal of Engineering Research (AJER)
e-ISSN : 2320-0847 p-ISSN : 2320-0936
Volume-04, Issue-01, pp-01-07
www.ajer.org
Research Paper Open Access

"Distinct Revocable Data Hiding In Ciphered Image"

Anamika Patil[1], Mona Pounikar[2], Pooja Bafna[3], Pranjal Badgujar[4]
[1](Computer, University of Pune, India)[2](Computer, University of Pune, India)
[3](Computer, University of Pune, India)[4](Computer, University of Pune, India)

ABSTRACT: *This scheme proposes an authenticated and secure reversible data hiding in cipher images. Nowadays, more attention is paid to reversible data hiding in encrypted images, as the original cover can be reversibly recovered after embedded data is retrieved. In the first stage, the content owner encrypts the original image using an encryption key. Then, a data hider compresses the least significant bits (LSB's) of the encrypted image using a data hiding key to create space to store some additional data. Then, if a receiver has the data hiding key, he can extract the additional data from the encrypted image though he is unaware of the image content. If the receiver has the encryption key with him, then he can decrypt the data to obtain an image similar to the original image. If the receiver has both the data hiding key as well as the encryption key, then he can extract the additional data as well as he can recover the original content.*

KEYWORDS: *Encryption, Steganography, Data Hiding.*

I. INTRODUCTION

Distinct revocable data hiding in ciphered image also means hiding data reversibly in encrypted image in separable manner. Nowadays data transmission over internet has increased tremendously so image security has become an important factor to be considered for e.g., video surveillance, confidential transmission, medical and military applications. As in medical field the necessity of fast and secure diagnosis is important in the medical world. To reduce the transmission time over network, the data compression is necessary. In the current trends of the world, the technologies have advanced and emerged so much that most of the individuals prefer using the internet as the primary medium to transfer data from one end to another across the world. There are many possible ways to transmit data using the internet: via emails, chats, etc. The data transition is made very simple, fast and accurate using the internet. However, one of the major problem with sending data over the internet is the security threat it poses i.e. the secret or personal data can be stolen or hacked in many ways. Therefore it is very important to take data security into consideration and a matter of concern, as it is one of the most essential factors that need attention during the process of data transferring. The protection of this multimedia data can be done with data hiding and encryption algorithms. In the current trends of the world, the technologies have advanced so much that most of the individuals prefer using the internet as the primary medium to transfer data from one end to another across the world. There are many possible ways to transmit data using the internet through emails, chats or other means.

Data security basically means protection of data from unauthorized users or hackers and providing high security to prevent data being modified. Therefore area of data security has gained more attention over the recent period of time due to the massive increase in data transfer rate over the internet. In order to improve the secret communication and security features in data transfers over the internet, many efficient techniques have been developed like: Cryptography and Steganography.Reversible data hiding (RDH) in images is a technique, in which we can recover the original cover losslessly after the embedded message is extracted. In order to provide security and privacy for images, encryption is an effective and popular means as it converts the original content to incomprehensible one which is not understood. There are some promising applications in RDH that can be applied to encrypted images. The process of extracting data from image requires compression of encrypted images and space for data embedding. Compression of encrypted data can be considered as source code with some information at the decoder, in which the practical method is to generate the compressed data in reversible manner by exploiting the syndromes of parity-check matrix of channel codes [4].In practical aspect, many RDH techniques have evolved in recent years which are helpful in many ways. A general framework have been constructed for RDH. By first extracting compressible features of original image and then compressing them losslessly,

spare space can be created for embedding data. A more efficient method is dependent on difference expansion (DE) [5], in that the difference of each pixel group is expanded, and the least significant bits (LSBs) of the difference are all zero and can be used for embedding messages and data. The motivation of reversible data embedding can be considered as distortion-free data embedding. Though embedding some data will inevitably change the original content. Even a very small change in pixel values may not be desirable, especially in sensitive images, such as military and medical data. In such situations, every bit of information is important to be considered. Even a small change is going to affect the intelligence of the image, and the access to the original data is always required.

II. REVOCABLE DATA HIDING

Revocable data hiding also known as Reversible data hiding in images is a method that hides data in digital images for secret and secured communication through network. It is a technique to hide additional data into cover media in a reversible way so that the original cover content can be perfectly and accurately recovered after extraction of the hidden data. Traditionally, data hiding is used for secret and secured communication. In many applications that we use, the embedded carriers are encrypted so as to prevent the carrier from being analyzed to reveal the presence of the embedded information. Other applications could be used when the owner of the carrier might not want the other unauthorized person, including data hider, to know and reveal the content of the carrier before data hiding is actually done, such as military or confidential medical images. A major trend is minimizing the computational requirements for secure and secret multimedia distribution by selective encryption where only parts of the data are encrypted. Two levels of security are there for digital image encryption, they are: low level and high-level security encryption. In case of low level security encryption, the image which is encrypted has low visual quality compared to that of the original one, but the content of the image is still visible and easily understandable to the users. In the high-level security encryption, the content of image is completely scrambled and the image will be in random noise format. In this case, the image is not easily understandable to the users at all. Selective encryption aims at avoiding the encryption of all bits of a digital image and also ensures a secure encryption standard [5].

In our proposed method, we first empty out the memory space by embedding LSBs of some pixels into other pixels with a traditional RDH method and then apply encryption on the image, so the positions of these LSBs in the encrypted image can then be used to embed data. Not only does the proposed method separate data extraction from image decryption but also it achieves better performance in a different prospect that is real reversibility is realized, so that we can say data extraction and image recovery are error free. Most of the work on reversible data hiding focuses on the data embedding and data extracting on the plain spatial domain. But, in some applications, the administrator appends some additional message, such as the source information, notation of image or authentication data, inside the encrypted image though he does not know the original image content. And also it is hopeful that the original content should be recovered without any error after image decryption and message extraction on receiver side, that is, the original content must be error free.Reversible data embedding is a secret and secured communication channel since reversible data embedding can be used as a data carrier. Reversible data embedding, which is also called lossless data embedding, embeds data into a digital image in a reversible way. Interesting feature of reversible data embedding is the reversibility that is we can remove the embedded data so as to recover the original image. Reversible data embedding hides some data in a digital image in such a way that any authorized party can decode the hidden information and also recover the image to its original state.

III. EXISTING SYSTEM

In reversible data hiding method the image is compressed and encrypted by using the encryption key. The data to be hidden is embedded inside image by using the data hiding key. At the receiver end, the receiver first need to extract the image using the encryption key in order to extract the data and in order to extract the embedded data he will use a data hiding key. It is a serial process and is not a separable process. Steganography is said to be the art and science of writing hidden messages in such a way that no one, except for the sender and the authorized recipient, can detect the existence of the message. The word Steganography is evolved from Greek origin and it means "covered writing" meaning” protected", Usually, messages will appear to be something else like images or articles or shopping lists, the hidden message may be considered to be invisible ink between the visible lines of a private letter. It is a secure technique for long and secret data transmission. Steganography is the process of hiding some information into other sources of information like text or image so that it is not easily visible to the natural view. Any other person cannot recognize it. There are varieties of stenographic techniques that are available to hide the data depending upon the carriers that we are going to use.

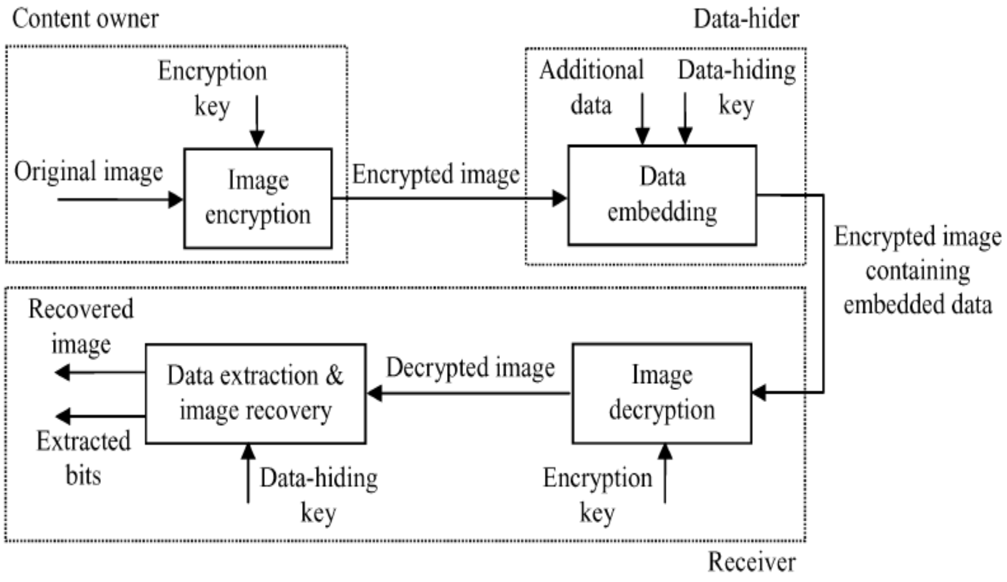


Fig. 1. Sketch of non-separable reversible data hiding in encrypted image.

In the existing system, the image is initially compressed and encrypted using the encryption key and the data which is to be hidden is embedded in to the image using the data hiding key. A content owner encrypts the original image by using an encryption key, the data-hider can then embed additional data into the encrypted image using a data-hiding key though he is not aware about the original one. An encrypted image that contains additional data, a receiver must first decrypt the image according to the encryption key, and then he can extract the additional embedded data and thus recover the original image according to the data-hiding key [2]. In this scheme data extraction is not separable from data decryption. In other way we can say that, the additional data must be extracted from the image which is decrypted, in order to know the principal content of original image before data extraction, and, if anyone does not have the data-hiding key but have the encryption key, then he cannot extract any data from the encrypted image containing additional data but he can decrypt the image as shown in Fig 1.

Disadvantages: The principal content of the image is revealed prior to data extraction.
If anyone has the data hiding key but not the encryption key then he cannot obtain any information from the encrypted image containing additional data.

IV. PROPOSED SCHEME

Our system will have some new features so as to overcome the above issues. Transactions will occur in a secured format between various clients over network. It provides flexibility to the user to transfer the data through the network very easily by compressing the large data in file. It will also recognize the user and provide the communication according to the security standards. The user who is going to receive the file will do the operations like de-embedding, decryption, and uncompressing in their level of hierarchy and get the information which is required. Compressing the data will increase the performance of data transfer and embedding the encrypted data will assure the security while the transferring data over network.

The proposed scheme consists of image encryption, data embedding and data-extraction or image-recovery. The content owner first encrypts the original image using an encryption key to obtain an image in encrypted form. The data-hider compresses the least significant bits (LSB) of the encrypted image using a data-hiding key in order to create a sparse space to accommodate some more amount data. Now at the receiver side, the data embedded in the created space can be easily retrieved according to the data hiding key from the encrypted image. Because the data embedding only affects the LSB, a decryption using an encryption key can then give us an image similar to the original one. By using both the encryption as well as the data-hiding key, the embedded additional data can be successfully retrieved and also the original image can be perfectly recovered [2].

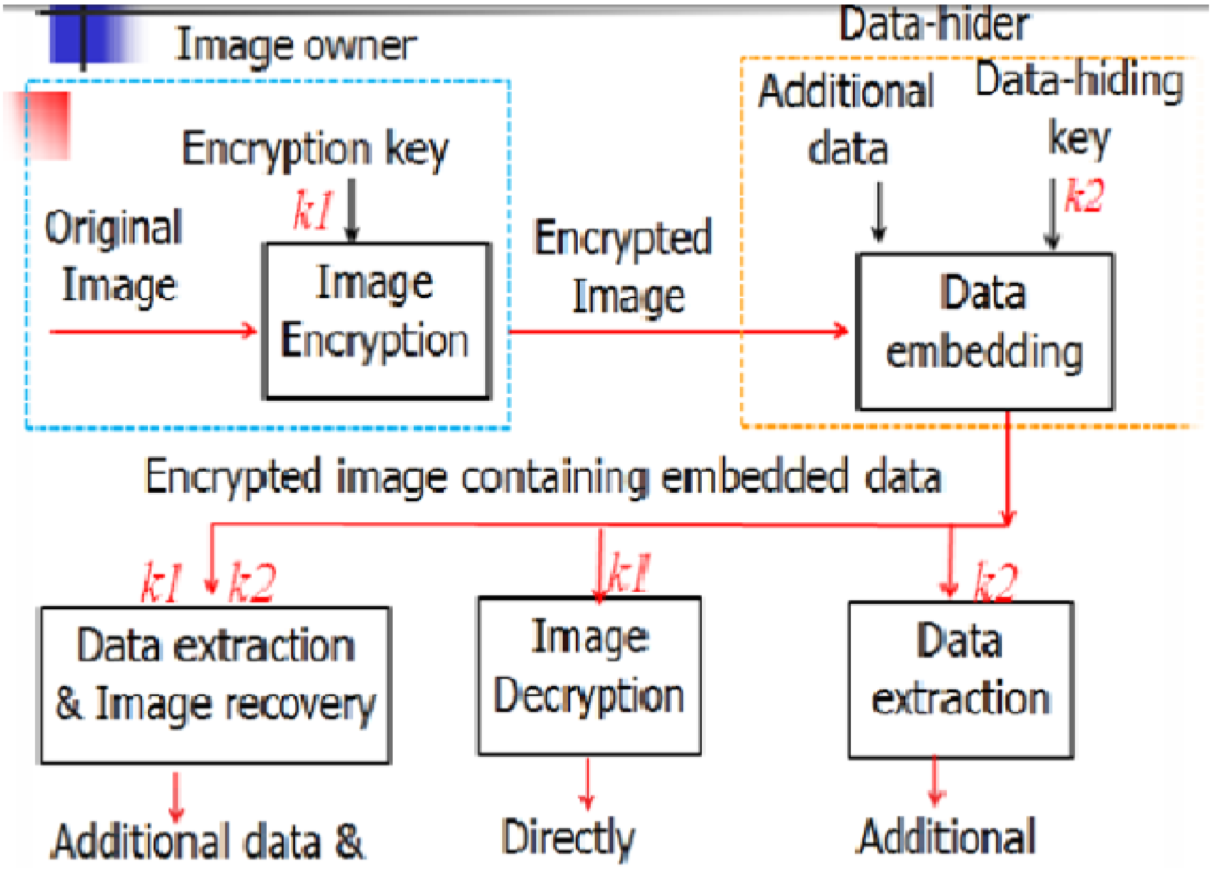


Fig 2. Separable reversible data hiding in encrypted image

This paper proposes a method for distinct revocable data hiding in ciphered image. As shown in Fig. 2, the content owner initially reserve enough space on original image to embed data and then by using an encryption key image is converted into its encrypted form. The data embedding process in encrypted images is inherently reversible for the data hider as he only needs to accommodate data into the created space. The data extraction phase and image recovery phase are similar to that of Framework Vacating room after encryption. In the new framework, we follow the idea that first losslessly compresses the redundant image content and then encrypts in order to protect privacy and maintain security. Next, we consider a practical method based on the Framework “Reserving room before encryption”, that has four stages as follows: creating an encrypted image, data hiding in encrypted image, data extraction and image recovery.

Advantages: If the receiver only has the data-hiding key, he can extract the additional data also if he does not know the image content. If he has only the encryption key and not the data hiding key he can decrypt the received data to obtain an image similar to the original image, as data hiding key is absent he cannot extract the additional data. If he receiver has both the data-hiding key as well as the encryption key, can extract the additional data and also recover the original image without any error when the additional data is not too large.

V. IMAGE ENCRYPTION

The user will initially browse the image and encrypt the image, then the system will auto generate an encryption key for encryption. Encryption applies special mathematical algorithms and keys so as to transform digital data into cipher text before they are transmitted further and then decryption applies mathematical algorithms and keys to get back the original data from cipher text. As information privacy becomes a challenging issue thus in order to protect valuable and secret data or image from unauthorized users, data or image encryption or image decryption is important. Consider an original image with a size of Q1 * Q2 which is in uncompressed format and each pixel with gray value falling into [0, 255] is represented by 8 bits. We can denote the bits of a pixel as bij0, bij1,....bij7 where 1<i<Q1 and 1<j<Q2, represent the gray value as P i ,j and the number of pixels as Q (Q= Q1 * Q2). In encryption phase, we calculate the pseudo-random bits and original bits exclusive-or results, where

$$B_{i,j,u} = b_{i,j,u} \oplus r_{i,j,u}$$

r, i, j, u can be determined by using an encryption key. Then B, i, j, u, are concatenated in an ordered manner as in encrypted data.

VI. DATA EMBEDDING

User will hide the encrypted data in encrypted image and system will then automatically generate data hiding key. In the data embedding stage, we embed few parameters into a small number of encrypted pixels, and the LSB of the other encrypted pixels are compressed to create a sparse space for so that we can accomodate the additional data and the original data at the positions obtained by the parameters. The data-hider will randomly select Np encrypted pixels using a data hiding key that will be used to carry the parameters for data hiding. Np is a small positive integer, for example, Np=20. The remaining (N-Np) encrypted pixels are permuted and divided into a number of groups, each group will contain L pixels. We can determine the permutation way by using the data-hiding key. For each pixel-group, for L pixels select the M least significant bits, and represent them as B (k,1) , B (k,2) B(k, M*L) where k represents a group index within [1,(N-Np)/L] and M represents a positive integer less than 5. The data-hider generates a matrix G, which is made up of two parts. The left part represents identity matrix and the right part represents pseudo-random binary matrix which is obtained from the data-hiding key. Now for each group, which is product with the G matrix to form a matrix of size (M * L-S), that has a sparse bit of size S, in which the data is embedded and the pixels are then arranged into the original form and re-permutated to form an original image.

$$\begin{bmatrix} B'(k,1) \\ B'(k,2) \\ \vdots \\ B'(k, ML-S) \end{bmatrix} = \mathbf{G} \cdot \begin{bmatrix} B(k,1) \\ B(k,2) \\ \vdots \\ B(k, ML) \end{bmatrix}$$

VI. IMAGE DECRYPTION

The user will first browse data that he wish to send to receiver and then encrypt the original data and the system will auto generate the data encryption key.The content owner encrypts the original image using an encryption key. Even if the data-hider does not know the original content, he can easily compress the least significant bits of the encrypted image using a data-hiding key to create some space so as to accommodate the additional data. Now with an encrypted image containing additional data, by using a data hiding key receiver can obtain the additional data, or obtain an image similar to the original one using only the encryption key. When the receiver has both of the keys with him, he can extract the additional data as well as he can recover the original content without any error. When having an encrypted image containing embedded data, using encryption key receiver first generate ri,j,k, and calculates the exclusive-or of the received data and ri,j,k so as to decrypt the image. We can denote the decrypted bits as bri,j,k. The original most significant bits (MSB) are retrieved correctly without any errors. Now for a certain pixel, if the embedded bit which is in the block including the pixel is zero and the pixel is belonging to D1, or if the embedded bit is 1 and the pixel is belonging to D0, then the data-hiding will not affect any encrypted bits of the pixel. So, the three LSB which are decrypted must be same as the original LSB, which implies that the decrypted gray value of the pixel is correct. In other way, if the embedded bit in the pixels block is zero and the pixel is belonging to D0, or the embedded bit is one and the pixel is belonging to D1, the decrypted LSB.

$$\begin{aligned} b'_{i,j,k} &= r_{i,j,k} \oplus B'_{i,j,k} \\ &= r_{i,j,k} \oplus \overline{B_{i,j,k}} \\ &= r_{i,j,k} \oplus \overline{b_{i,j,k} \oplus r_{i,j,k}} \\ &= \overline{b_{i,j,k}}, \qquad k = 0,\ 1,\ 2. \end{aligned}$$

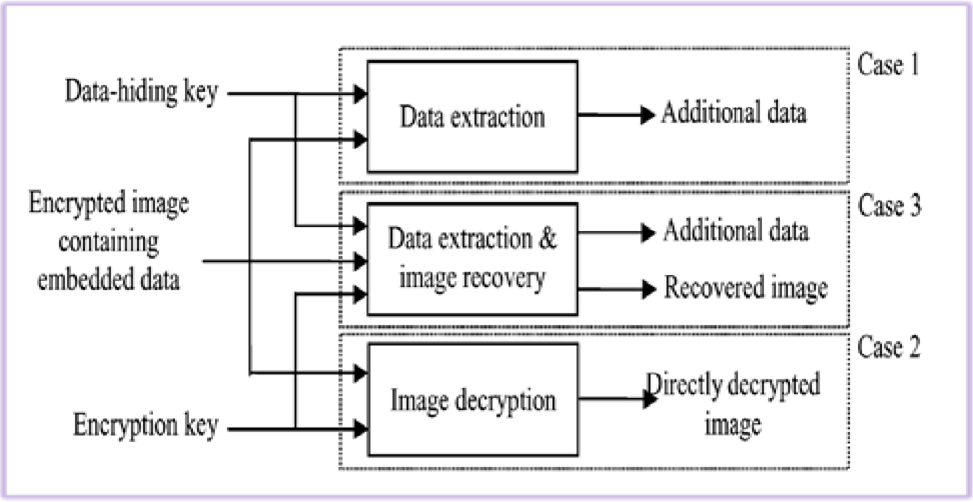
VIII. DATA EXTRACTION

As data extraction is totally independent from image decryption, their order implies two different practical applications which are as follows:

First case: Extracting Data from Encrypted Images*:* In order to update some personal information of images which are encrypted for protecting privacy, the database manager will only get access to the data hiding key and will have to calculate data in encrypted domain. Order of data extraction before image decryption will guaranty the feasibility of our work. When the database manager will obtain the data hiding-key, so he will be able to decrypt the LSB-bits of encrypted image of A which is denoted by AE, and then obtain the additional data z by directly reading the decrypted image. When we request for updating information of encrypted images, the database manager, will then update information through LSB replacement and will encrypt updated information according to the data hiding key. Now the entire process is completely operated on encrypted domain, so it will avoid the leakage of original data.

Second case: Extracting Data from Decrypted Images: In 1, embedding and extraction of the data both are calculated in encrypted domain. In other way, there is another situation that the user will want to decrypt the image first and then obtain the data from the decrypted image when it will be required. The following example illustrates an application for such scenario. Consider Alice outsourced her images to a cloud server, and the images are encrypted in order to protect their data into the encrypted images, by embedding some notation the cloud server will mark the images, by including the identity of the images owner and the identity of the time stamps and the cloud server, so as to manage the encrypted images. The cloud server has no authority to do any kind of permanent damage to the images. Only an authorized user, Bob who has the encryption key and the data hiding key with him, downloaded the images and then he decrypted the images. Bob marks decrypted images, so that decrypted images will include the notation, this notation can be used to trace the history and origin of the data. Order of image decryption before data extraction or without data extraction is suitable in this case.

If the receiver has both the data-hiding key and encryption key, he may hope to obtain the embedded data. Now according to the data-hiding key, the values of M,S and L, the LSB of the Np selected encrypted pixels, and the (N-Np) * S/L - Np additional bits can then be obtained from the encrypted image which containing embedded data. Now by placing the Np LSB into their original positions, the data which is encrypted of the Np selected pixels are retrieved, using the encryption keys their original gray values can be appropriately decrypted. We will recover the original gray values of the other (N-Np) pixels. This paper proposes a novel scheme for distinct revocable data hiding, that is, separable reversible data hiding in encrypted image.



In the proposed scheme, by using an encryption key we can encrypt the original image and by using a data hiding key the additional data can be added in to the encrypted image. Now along with an encrypted image containing additional data, if the receiver only has the data-hiding key, then he can only extract the additional data embedded inside the image even if he is not aware about the image content. If the receiver only has the encryption key, and not the data hiding key then he can decrypt the received data to obtain an image similar to the original image, but then he cannot extract the additional data. In other case, if the receiver has both the data-hiding key as well as the encryption key, then he can obtain the additional data and also recover the original image content without any error when the amount of additional data is considerably small.

IX. CONCLUSION AND FUTURE SCOPE

In this paper, we have proposed a novel scheme for distinct revocable data hiding in ciphered image which consists of 3 phases: image encryption, data embedding and data-extraction or image recovery. In the first stage, the content owner encrypts the original image using an encryption key. Although a data-hider does not know the original content, he can compress the least significant bits of the encrypted image using a data-hiding key so as to create a sparse space to embed the additional data into the encrypted image. With an encrypted image containing additional data, the receiver can extract the additional data using only the data hiding key, or obtain an image exactly similar to the original image using the encryption key. When the receiver has both the keys, the data hiding key as well as encryption key, he can extract the additional data and also recover the original content. If the lossless compression method is used for the encrypted image which contains embedded data, the additional data can still be extracted and the original content can be also recovered since the lossless compression does not change the content of the encrypted image containing embedded data.The reversible compression method is used for the encrypted image containing embedded data, the additional data can be extracted and the original content can be also recovered since the lossless compression does not change the content of the encrypted image containing additional data. Reversible data hiding in encrypted images is a new concept which attracts our attention due to the privacy-preserving requirements from cloud data management. This study helps constructing secure and secret transmission of secrete file in order to prevent any unauthorized party access information and security level of data is increased by encrypting data. We also provide protection for keys during decryption process so that even if any hacker attacks on system it should be secure. In further future we can also use video, audio in case of image as cover for data hiding.

X. ACKNOWLEDGEMENTS

We wish to thank the Department of computer of MET BKC IOE College Nasik for providing the materials and their support during the course of this work.

REFERENCES

[1] Study on Separable Reversible Data Hiding in Encrypted Image, International Journal of Advancements in Research & Technology, Volume 2, Issue 12, December-2013 223 ISSN 2278-7763.

[2] Xinpeng Zhang, Separable Reversible Data Hiding in Encrypted Image**,** IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, NO. 2, APRIL 2012.

[3] Kede Ma, Weiming Zhang, Xianfeng Zhao, *Member, IEEE*, 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.

[4] Lalit Dhande, Priya Khune, Vinod Deore, Dnyaneshwar Gawade, Hide Inside-Separable Reversible Data Hiding in Encrypted Image, International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-3, Issue-9, February 2014.

[5] Jun Tian, Reversible Data Embedding Using a Difference Expansion, IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 13, NO. 8, AUGUST .

[6] 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.

[7] C.-C. Chang, C.-C. Lin, and Y.-H. Chen, Reversible data-embedding scheme using differences between original and predicted pixel values, IET Inform. Security, vol. 2, no. 2, pp. 35–46, 2008.

[8] Kede Ma, Weiming Zhang, Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption, IEEE Trans. VOL. 8, no. 3, Mar 2013.