ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

Separable Reversible Data Hiding with Data Security

Chinchu Lipson [1], Lipson Chirayath[2]

Technical Manager, Pursued M.Tech, Dept. of CSE, Bharath University, Chennai, India [1]

Technical Manager, Pursued B.Tech, Dept. of IT, Vinayaka Mission University, Salem, India [2]

ABSTRACT: Reversible data hiding (RDH) in images is an important technique, by which the original image can be losslessly recovered after the embedded data is extracted while protecting the image content's confidentiality. This paper proposes a novel scheme for separable reversible data hiding in encrypted images. In the first phase, a content owner encrypts he original uncompressed image using an encryption key. Then, a data-hider may compress the least significant bits of the encrypted image using a data-hiding key to create a sparse space to accommodate some additional data. With an encrypted image containing additional data, if a receiver has the data-hiding key, he can extract the additional data though he does not know the image content. If the receiver has the encryption key, he can decrypt the received data to obtain an image similar to the original one, but cannot extract the additional data. If the receiver has both the data-hiding key and the encryption key, he can extract the additional data and recover the original content.

KEYWORDS: Reversible data hiding, data embedding, image encryption, privacy protection, sharing process, image decryption, data extraction.

I. INTRODUCTION

In the current trends of the world, the technologies have advanced so much that most of theindividuals prefer using the internet as the primary medium to transfer data from one end toanother 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 main problems with sending data over the internet is the security threat itposes i.e. the personal or confidential data can be stolen or hacked in many ways. Therefore itbecomes very important to take data security into consideration, as it is one of the most essentialfactors that need attention during the process of data transferring.

Nowadays, more and more attention is paid to reversible data hiding (RDH) [2] in encrypted images since it maintains the excellent property that the original image can be losslessly recovered after the embedded data is extracted. There are also a number of works on data hiding in the encrypted domain. This technique is widely used in medical imagery, military imagery and law forensics, where no distortion of the original image is allowed. Since first introduced, RDH has attracted considerable research interest.

Most of the work on reversible data hiding focuses on data embedding/extracting on the encrypted images. The rapid development of data transfer through internet made it easier to send the data accurateand faster to the destination. There are many transmission media to transfer the data todestination like e-mails; at the same time it is may be easier to modify and misuse the valuableinformation through hacking. So, in order to transfer the data securely to the destination withoutany modifications, there are many approaches like cryptography and steganography. This paperdeals with the image steganography as well as with the different security issues, generaloverview of cryptography approaches and about the different steganographic algorithms likeLeast Significant Bit (LSB) algorithm [15], JSteg, F5 algorithms. It also compares thosealgorithms in means of speed, accuracy and security.

Separable reversible data hiding is very useful for some extremely image such like medical images and military images. In the reversible data hiding schemes, some schemes are good performance at hiding capacity but have a bad stego image quality, some schemes are good stego image quality but have a low hiding capacity. It is difficult to find the balance between the hiding capacity and stego image quality. Data security basically means protection of data from unauthorized users or hackers andproviding high security to prevent data modification. This area of data security has

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

gained moreattention over the recent period of time due to the massive increase in data transfer rate over theinternet. In order to improve the security features in data transfers over the internet, manytechniques have been developed like: Cryptography, Steganography [13]. While Cryptography is amethod to conceal information by encrypting it to cipher texts and transmitting it to theintended receiver using an unknown key, Steganography provides further security by hiding thecipher text into a seemingly invisible image or other formats.

In theoretical aspect, Kalker and Willems [14] established a rate-distortion model for RDH, through which they proved the rate-distortion bounds of RDH for memory less covers and proposed a recursive code construction which, however, does not approach the bound. Zhang [2], [6] improved the recursive code construction for binary covers and proved that this construction can achieve the rate-distortion bound as long as the compression algorithm reaches entropy, which establishes the equivalence between data compression and RDH for binary covers.

In practical aspect, many RDH techniques have emerged in recent years. Fridrich [9] constructed a general framework for RDH. By first extracting compressible features of original cover and then compressing them losslessly, spare space can be saved for embedding auxiliary data. A more popular method is based on difference expansion (DE) [5], in which the difference of each pixel group is expanded, e.g., multiplied by 2, and thus the least significant bits (LSBs) of the difference are all-zero and can be used for embedding messages. Another promising strategy for RDH is histogram shift (HS) [7], in which space is saved for data embedding by shifting the bins of histogram of gray values. The state-of-art method [10]-[13] usually combined DE or HS to residuals of the image, e.g., the predicted errors, to achieve better performance.

Some attempts on RDH in encrypted images have been made. Zhang in [5] divided the encrypted image into several blocks. By flipping 3 LSBs of the half of pixels in each block, room can be vacated for the embedded bit. The data extraction and image recovery proceed by finding which part has been flipped in one block. This process can be realized with the help of spatial correlation in decrypted image.

All the above methods follows the reversible data hiding technique like that firstly the image is compressed [3] andencrypted by using the encryption key and the data to hide is embedded in to the image by usingthe data hiding key. At the receiver side he first need to extract the image using the encryptionkey in order to extract the data and after that he'll use data hiding key to extract the embeddeddata. It is a serial process and is not a separable process.This proposed method also achieves excellent performance in three different prospects.

- •Real reversibility is achieved, that is, data extraction and image recovery are free of any error.
- •Extra security is realized, that is, unauthorized access is mostly restricted
- •Data extraction and image recovery can be separate.

This paper is organized in the following manner. Section II briefly introduces previous methods proposed in [3]-[5]. The novel method is elaborated in Section III in. Experiments set up and comparisons are given in Section IV. The paper is concluded in Section VI.

II. RELATED WORKS

The methods proposed in [3]-[5] all the above papers can be summarized as the framework, as illustrated in Fig. 1.In this framework, a content owner encrypts the original image using a standard cipher with an encryption key. After producing the encrypted image, the content owner hands over it to a data hider (e.g., a database manager) and the data hider can embed some auxiliary data into the encrypted image by losslessly vacating some room according to a data hiding key. Then a receiver, maybe the content owner himself or an authorized third party can extract the embedded data with the data hiding key and further recover the original image from the encrypted version according to the encryption key .

In all the above methods of [3]-[5], the encrypted 8-bit gray-scale images are generated by encrypting every bit-plane with a stream cipher. The method segments the encrypted image into a number of nonoverlapping blocks sized by n x n; each block is used to carry one additional bit. To do this, pixels in each block are pseudo randomly divided into two sets S_1 and S_2 according to a data hiding key. If the additional bit to be embedded is 0, flip the 3 LSBs of each encrypted pixel in S_1; otherwise flip the 3 encrypted LSBs of pixels in S_2. For data extraction and image recovery, the receiver flips all the three LSBs of pixels in S_1 to form a new decrypted block, and flips all the three LSBs of pixels in S_2 to form another new block; one of them will be decrypted to the original block. Due to spatial correlation in natural images, original block is presumed to be much smoother than interfered block and embedded bit can be extracted

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

correspondingly. However, there is a risk of defeat of bit extraction and image recovery when divided block is relatively small or has much fine-detailed textures. All the existing methods are used cryptography concept only for hiding the content of the messages, not to hide the existence of the messages.To hide the data in particular bit they are using public key, so which can be easily extract the original messages.The receiver decrypts the original image and embedded data using the single key only. It is a serial process too.Hong [4] reduced the error rate of Zhang's [5] method by fully exploiting the pixels in calculating the smoothness of each block and using side match.

The extraction and recovery of blocks are performed according to the descending order of the absolute smoothness difference between two candidate blocks and recovered blocks can further be used to evaluate the smoothness of unrecovered blocks, which is referred to as side match.Zhang's [3] method is pseudo randomly permuted and divided encrypted image into a number of groups with size of L. The P LSB-planes of each group are compressed with a parity-check matrix and the vacated room is used to embed data.

III. PROBLEM STATEMENT

Since losslesslyextractingdata from the encrypted images is relatively difficult and sometimes inefficient. If we change the serial order of compressing and encrypting the original image, the RDH tasks in encrypted images would be more natural and much easier which leads us to the novel framework, "separable reversible data hiding" [1].

As shown in Fig. 2, the content owner first encrypts the original image by using the encryption key. Now, the data embedding process in images is inherently reversible. For the data hider only needs to compress the Least Significant Bit (LSB) and accommodate data into the spare space generated using data hiding key. Then the image with embedded data is transmitted. Here we use visual cryptography algorithm to encrypt the image and to embed data. The data extraction and image recovery are separable. Obviously, standard RDH algorithms are the ideal operator for achieving better performance compared with techniques from previous framework. This is because in this new framework, we follow the customary idea that first encrypting the image and embedding the secret data to the spare spaces generated by compressing the LSB bits, with respect to protecting privacy.

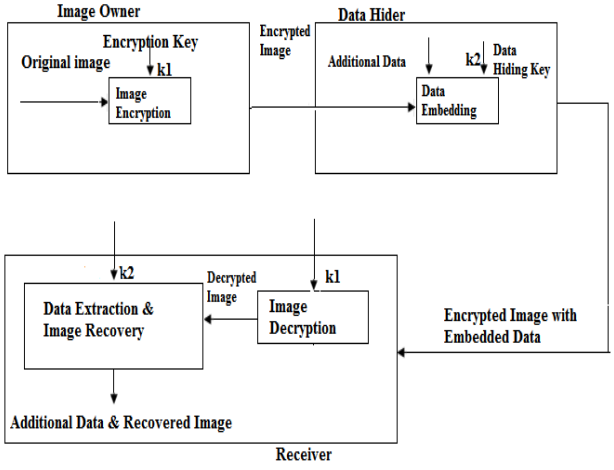

Fig. 1. (a) Existing Framework

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

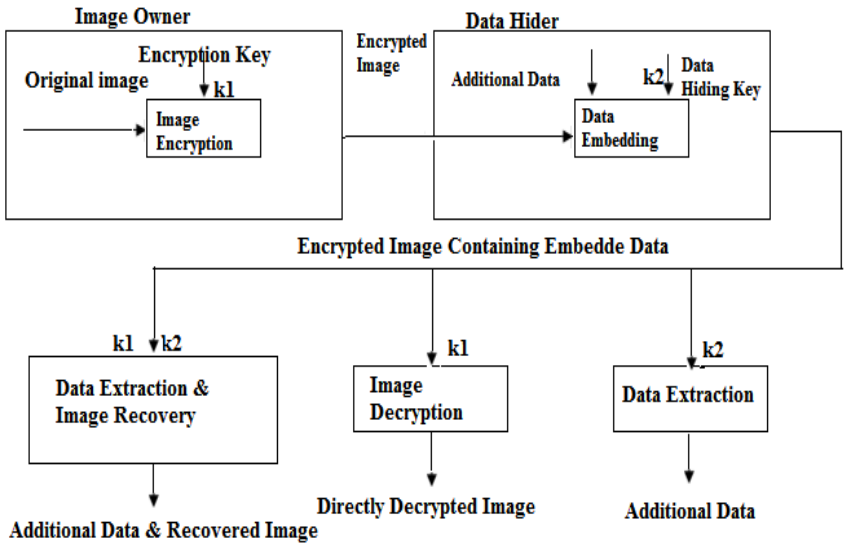

Fig. 2. Proposed Framework

Next we elaborate the practical method based on the proposed framework, which primarily consists of three stages: image encryption, data embedding, data extraction and image recovery.

A. Image Encryption

In recent years, the advances in communication technology have seen strong interest in digital image transmission. However, growth of computer processor possessing power and storage illegal access has become easier. Encryption involves applying special mathematical algorithms and keys to transform digital data into cipher code before they are transmitted and decryption involves the application of mathematical algorithms and keys to get back the original data from cipher code, scientific community have seen strong interest in image transmission. However, illegal data or image access has become more easy and prevalent in wireless and general communication networks. Information privacy becomes a challenging issue. In order to protect valuable data or image from undesirable readers, data or image encryption /decryption [2] is essential, furthermore. As such in this paper, a scheme based on encryption has been proposed for secure image transmission over channels as shown in Fig. 3..

Around 70% of the information transmission on digital images is over the internet, which is an important parts of network exchanges. However, the image information, which is different fromtext message, has larger scale of data, higher redundancy and stronger correlation betweenpixels.Traditional encryption algorithms such as AES, IDES, are against the text messages to beproposed, which are not suitable for digital image encryption, therefore, an reliable digital imagewith characteristics is in urgent need of the encryption scheme DES is suitable for imageencryption, and decryption with is closely related to some dynamics of its own characteristics.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

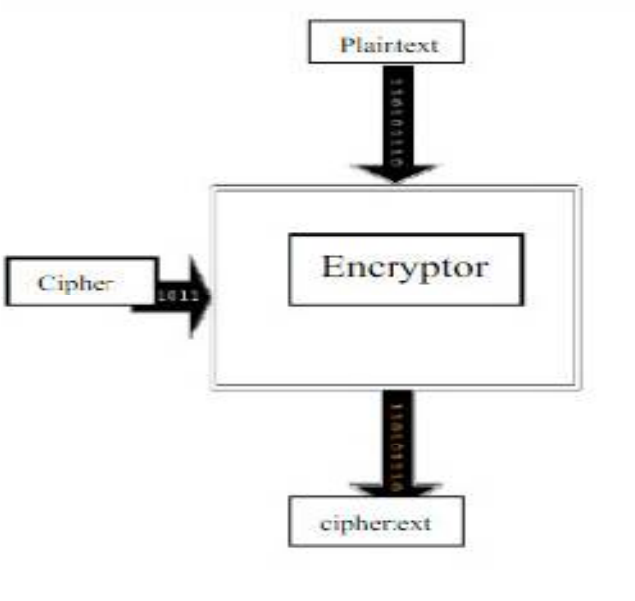

Fig. 3. General Encryption Mechanism

The DES algorithm [6] gains wide application in our daily life, such as smart cards, cell phones,automated teller machine sand WWW servers. DES encrypts a plaintext to become a cipher text,which can be decrypted back to the original plaintext by using common key, an example isshown in Figure 2. It can be seen the cipher text is very different from and gives no clue to theoriginal plaintext. Figure shows the Encryption of DES operation using cipher key.Assume the original image with a size of N1 * N2 is in uncompressed format and each pixel withgray value falling into [0, 255] is represented by 8 bits. Denote the bits of a pixel as$b_{i,j,0}$, $b_{i,j,1}$…$b_{i,j,7}$ where$1 \leq i \leq N1$ and $1 \leq j \leq N2$, the gray value as $P_{i,j}$ and the numberof pixels as N (N= N1 * N2). In encryption phase, the exclusive-or results of the original bits and pseudo-random bits arecalculated.

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

where$r_{i,j,u}$are determined by an encryption key using a standard stream cipher. Then, $B_{i,j,u}$areconcatenated orderly as the encrypted data.

B. *Data Embedding*

Once the data hider acquires the encrypted image, he can embed the secret data into the places which we are generated by compressing the Least Significant Bits in the pixels. The embedding process starts with locating the places to embed data. After compressing the bits, the spare space can be utilized to accommodate secret data. Then the data hider simply adopts LSB replacement to substitute the available bit-planes with additional data. Finally, the data hider sets a label following the embedded data to point out the end position of embedding process. Anyone who does not possess the data hiding key could not extract the additional data.

In the data embedding phase, some parameters are embedded into a small number of encryptedpixels, and the LSB of the other encrypted pixels are compressed to create a space foraccommodating the additional data and the original data at the positions occupied by theparameters. The detailed procedure is as follows: - According to a data-hiding key, the data-hiderrandomly selects Np encrypted pixels that will be used to carry the parameters for data hiding.Here, Np is a small positive integer, for example, Np=20. The other (N-Np) encrypted pixels arepermuted and divided into a number of groups, each of which contains L pixels. The permutationway is also determined by the data-hiding key. For each pixel-group, collect the M leastsignificant bits of the L pixels, and denote them as B (k,1) , B (k,2) …… B(k,M*L)

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

where k is agroup index within [1,(N-Np)/L] and M is a positive integer less than 5.The data-hider alsogenerates a matrix G , which is composed of two parts. The left part is the identity matrix andthe right part is pseudo-random binary matrix derived from the data-hiding key. For each group,which is product with the G matrix to form a matrix of size (M * L-S). This has sparse bits of size S, in which the data is embedded and arrange the pixels into the original form and repermutated to form an original image.

There are many methods for steganography, to hide the secret message into the image. LSB is the well- known method for data hiding. The idea behind the LSB algorithm is to insert the bits of the hidden message into the least significant bits of the pixels.

C. Image Decryption and Data Extraction

The proposed paper provides a novel scheme for separable reversible data hiding in encrypted image. In the proposed scheme, the original image is encrypted using an encryption key and the additional data are embedded into the encrypted image using a data-hiding key. With an encrypted image containing additional data, if the receiver has only the data-hiding key, he can extract the additional data even though he does not know the image content. If he has only the encryption key, hecan decrypt the received data to obtain an image similar to the original one, but cannot extractthe embedded additional data. If the receiver has both the data-hiding key and the encryptionkey, he can extract the additional data and recover the original image without any error when theamount of additional data is not too large.Since data extraction is completely independent from image decryption, the order of them implies two different practical applications:-

1)Case 1&3:- Extracting Data From Decrypted Image

If the receiver has both the data-hiding and encryption key, or if the receiver has only the data hiding key, he may aim to extract the embedded data according to the data-hiding key. The values of M, L and S, the original LSB of the Np selected encrypted pixels, and the (N-Np) * S/L - Np additional bits can be extracted from the encrypted image containing embedded data. By putting the Np LSB into their original positions, the encrypted data of the Np selected pixels are retrieved, and their original gray values can be correctly decrypted using the encryption keys. In the following, we will recover the original gray values of the other (N-Np) pixels.

2)Case 2:- Extracting Data From Decrypted Images

In Case1&3, both embedding and extraction of the data are manipulated in encrypted domain. On the other hand, there is a different situation that the user wants to decrypt the image first and extracts the data from the decrypted image when it is needed. The following example is an application for such scenario. Assume Alice outsourced her images to a cloud server, and the images are encrypted to protect their contents. Into the encrypted images, the cloud server marks the images by embedding some notation, including the identity of the images' owner, the identity of the cloud server and time stamps, to manage the encrypted images. Now an authorized user, Bob who has been shared the encryption key and the data hiding key, downloaded and decrypted the images. Bob hoped to get marked decryptedimages, i.e., decrypted images still including the notation, which can be used to trace the source and history of the data. The order of image decryption before/without data extraction is perfectly suitable for this case. Next, we describe how to generate a marked decrypted image.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

(a) (b) (c) (d)

Fig. 4. Original Image Encrypted Version Decrypted Image Containing Messages Recovery Version

When having an encrypted image containing embedded data, a receiver firstly generates $r_{i,\ j,\ k}$according to the encryption key, and calculates the exclusive-or of the received data and$r_{i,\ j,\ k}$ todecrypt the image. We denote the decrypted bits as $br_{i,\ j,\ k}$. Clearly, the original five mostsignificant bits (MSB) are retrieved correctly. For a certain pixel, if the embedded bit in theblock including the pixel is zero and the pixel belongs to S1, or the embedded bit is 1 and thepixel belongs to S0, the data-hiding does not affect any encrypted bits of the pixel. So, the threedecrypted LSB must be same as the original LSB, implying that the decrypted gray value of thepixel is correct. On the other hand, if the embedded bit in the pixel's block is 0 and the pixelbelongs to S0, or the embedded bit is 1 and the pixel belongs to S1, the decrypted LSB.

IV. EXPERIMENT SETUP AND COMPARISONS

We have implemented the proposed framework using Java programming language. Java is developed by James Gosling at Sun Microsystems. We take standard image Lena, shown in Fig. 4(a), to demonstrate the feasibility of proposed method. Fig. 4(b) is the encrypted image containing embedded messages and the decrypted version with messages is illustrated in Fig. 4(c). Fig. 4(d) depicts the recovery version which is identical to original image.

We have compared the proposed method with the state-of- the-art works [1], [3]-[5]. As mentioned in Section I, all methods maybe introduce some errors on data extraction and/or image restoration, while the proposed method is free of any error for all kinds of images. In addition, another advantage of our approach is the much wider range of embedding rate for acceptable PSNRs. In fact, the proposed method can embed more than 5 times as large payloads for the same acceptable PSNR as the previous methods, which implies a very good potential for practical applications.We have compared the security of the proposed methods with the previous methods. The hacker didn't recover the embedded data because using the two separated keys i.e. data hiding keyfor embedding the content of message and encryption key for the existence of message by compressing the image.

V. CONCLUSION

In this paper, we propose a novel scheme for separable reversible data hiding in encrypted image, which consists of image encryption, data embedding and data-extraction/image recovery phases. In the first phase, the content owner encrypts the original uncompressed image using an encryption key. After that 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 to create a sparse space to accommodate the additional data. With an encrypted image with embedded data, the receiver may extract the additional data using only the data-hiding key, or obtain an image similar to the original one using only the encryption key. When the receiver has both of these keys, he can extract the additional data and recover the original image content without any error by exploiting the spatial correlation in natural image if the amount of additional data is not so large. If the lossless compression method is used for the encrypted image containing embedded data, the additional data can be still 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.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

REFERENCES

1. X. Zhang, "Reversible data hiding in encrypted images," IEEE SignalProcess. Lett., vol. 18, no. 4, pp. 255–258, Apr. 2011.
2. M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, "Oncompressing encrypted data," IEEE Trans. SignalProcess., vol. 52, no. 10, pp. 2992–3006, Oct.2004.
3. W. Liu, W. Zeng, L. Dong, and Q. Yao, "Efficient compression of encrypted gray scaleimages," IEEE Trans. Image Process., vol. 19, no. 4, pp. 1097–1102, Apr. 2010.
4. X. Zhang, "Lossy compression and iterative reconstruction for encrypted image," IEEETrans. Inform. Forensics Security, vol. 6, no. 1, pp. 53–58, Feb. 2011.
5. S. Lian, Z. Liu, Z. Ren, and H. Wang, "Commutative encryption and watermarking in videocompression," IEEE Trans. Circuits Syst. VideoTechnol., vol. 17, no. 6, pp. 774–778, Jun. 2007.
6. M. Cancellaro, F. Battisti, M. Carli, G. Boato, F. G. B. Natale, and A. Neri, "A commutativedigital image watermarking and encryption method in the tree structured Haar transformdomain," Signal Processing:Image Commun., vol. 26, no. 1, pp. 1–12, 2011.
7. D. Kundur and K. Karthik, "Video fingerprinting and encryption principles for digital rightsmanagement," Proceedings IEEE, vol. 92, no. 6, pp. 918–932, Jun. 2004.
8. J. Tian, "Reversible data embedding using a difference expansion,"IEEE Trans. CircuitsSyst. Video Technol., vol. 13, no. 8, pp. 890–896,Aug. 2003.
9. Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," IEEE Trans. Circuits Syst.Video Technol., vol. 16, no. 3, pp. 354–362, Mar.2006.
10. M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Lossless generalized-LSB dataembedding," IEEE Trans. Image Process., vol. 14, no.2, pp. 253–266, Feb. 2005.
11. W. Hong, T.-S. Chen, Y.-P.Chang, and C.-W. Shiu, "A high capacity reversible data hidingscheme using orthogonal projection and prediction error modification," Signal Process., vol. 90,pp. 2911–2922, 2010.
12. C.-C. Chang, C.-C.Lin, and Y.-H. Chen, "Reversible data-embedding scheme usingdifferences between original and predicted pixel values,"IET Inform. Security, vol. 2, no. 2, pp.35–46, 2008.
13. Kalker and F. M. Willems, "Capacity bounds and code constructions for reversible data-hiding," in Proc. 14th Int. Conf. Digital Signal Processing (DSP2002), 2002, pp. 71-76.
14. A. Mayache, T. Eude, and H. Cherifi, "A comparison of image quality models and metricsbased on human visual sensitivity," in Proc. Int.Conf. Image Processing (ICIP'98), Chicago, IL,1998, vol. 3, pp. 409–413.
15. Z. Wang and A. C. Bovik, "A universal image quality index," IEEE Signal Process.Lett.,vol. 9, no. 1, pp. 81–84, Jan. 2002
16. A. Sinha and K. Singh, "A technique for image encryption using digital signature," OpticsCommunications 218, pp. 229–234, 2003.
17. A. Lemma, S. Katzenbeisser, M. Celik, and M. van der Veen, "Secure WatermarkEmbedding through Partial Encryption," in International Workshop on Digital Watermarking(IWDW 2006), 4283, pp. 433–445, Springer Lecture Notes in Computer Science, 2006.

BIOGRAPHY

Chinchu Lipsonis currently working as a Technical Manager.She pursued her M.Tech in Computer Science & Engineering from Bharath University, Chennai. She received her B.Tech degree in CSE from IES College of Engineering, Calicut University, Kerala. She has 2 years of teaching and 3 years of industrial experience in the field of Information Technology.

Lipson Chirayathreceived his B.Tech degree in Information Technology from Vinayaka Mission University, Salem. He is having 14 years of experience in the field of Information Technology, Telecom, Networking, and Project Management. He is leading two IT related organizations with 100 employees. He has attended a variety of technological exhibitions, conferences in India and overseas. He has introduced latest trends in IT in his organizations to build up into core digital company.