Advanced Image Encryption System for Crime Investigation Applications

Chandana Roopa D[1], LekhaSree K[2], Divya Vani M[3], Kiran M[4], Jyothi T[5]

[1,2,3.4] U.G. Students, Department of ECE, Annamacharya institute of Technology and Sciences-Tirupati, A.P., India

[5] Assistant Professor, Department of ECE, Annamacharya institute of Technology and Sciences-Tirupati, A.P., India

Abstract **- Data security is essential for crime investigation applications. In these applications, all the evidences and details are stored in the format of images. Such image evidences are need to be secured to avoid the threats. For this purpose, we are going to implement advanced image encryption system. In existing method, we have seen the image encryption on key-based cryptography. There is a possibility for the criminals to hack the actual data with this technique. Hence, data security is low and also it is having low noise removable capacity. Since only one level of encryption is used, the values of SSIM and PSNR are also low. By introducing advanced image encryption system, we can provide high security for the data belongs to crime investigation departments. It includes two main techniques. Lossless data hiding by using cover image and reversible data hiding by using key based technique. By these techniques, we are going to improve the data security, such that cyber criminals cannot retrieve the original data. We are also going to improve the noise removal capacity, SSIM and PSNR values.**

Index Terms **- Image Encryption, Image Decryption, Cryptography.**

I.INTRODUCTION

Data security is essential for crime investigation applications. In these applications, all the evidences and details are stored in the format of images. Such image evidences are need to be secured to avoid the threats. For this purpose, we are going to implement advanced image encryption system. In existing method, we have seen the image encryption on key-based cryptography. There is a possibility for the criminals to hack the actual data with this technique. Hence, data security is low and also it is having low noise removable capacity. Since only one level of encryption is used, the values of SSIM and PSNR are also low. By introducing advanced image encryption system, we can provide high security for the data belongs to crime investigation departments. It includes two main techniques. Lossless data hiding by using cover image and reversible data hiding by using key based technique. By these techniques, we are going to improve the data security, such that cyber criminals cannot retrieve the original data. We are also going to improve the noise removal capacity, SSIM and PSNR values.

II.LITERATURE SURVEY

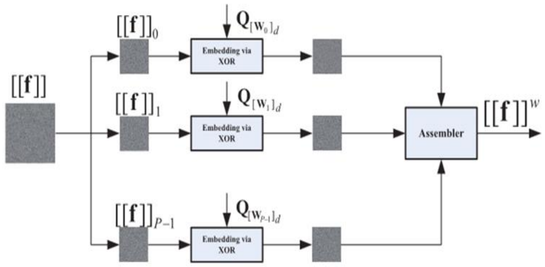

Fig. 1: Schematic of data hiding over encrypted domain

Instead of considering dedicated encryption algorithms tailored to the scenario of encrypted-domain data hiding, we here stick to the conventional stream cipher applied in the standard format. That is, the cipher text is generated by bitwise XORing the plaintext with the key stream. If not otherwise specified, the widely used stream cipher AES in the CTR mode (AES-CTR) is assumed. The resulting data hiding paradigm over encrypted domain could be more practically useful because of two reasons.

1) Stream cipher used in the standard format (e.g., AES-CTR) is still one of the most popular and reliable encryption tools, due to its provable security and high

software/hardware implementation efficiency. It may not be easy, or even infeasible, to persuade customers to adopt new encryption algorithms that have not been thoroughly evaluated.

2) Large amounts of data have already been encrypted using stream cipher in a standard way. When stream cipher is employed, the encrypted image is generated by

$[[f]] = Enc(f,K) = f \oplus K$ (1)

where and[[f]]denote the original and the encrypted images, respectively. Here, denotes the key stream generated using the secret encryption key K.

In this paper, without loss of generality, all the images are assumed to be 8 bits. Throughout this paper, we use[[x]]to represent the encrypted version of x. Clearly, the original image can be obtained by performing the following decryption function

$Dec = ([[f]],K) = [[f]] \oplus K.$ (2)

The schematic diagram of the proposed message embedding algorithm over encrypted domain is shown in Fig. 1. In this paper, we do not consider the case of embedding multiple watermarks for one single block, meaning that each block is processed once at most. For simplicity, we assume that the number of message bits to be embedded is n· A, Where A≤B and B is the number of blocks within the image. The steps for performing the message embedding are summarized as follows.

Step 1: Initialize block index i=1.

Step 2: Extractnbits of message to be embedded, denoted by Wi

Step 3: Find the public key Q[Wi]d associated with Wi, where the index [Wi] dis the decimal representation of Wi. For instance, when n=3andWi=010, the corresponding public key isQ2.

Step 4:Embed the length-n message bits Wi into the ith block via [[f]]wi=[[f]]i⊕Q[Wi]d.(6)

Step 5: Increment i=i+1 and repeat Steps 2–4 until all the message bits are inserted

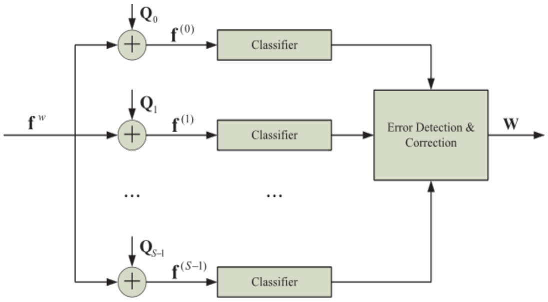

Fig. 2.Schematic of the data extraction

the proposed error correction approach is based on the following key observation: if a block is correctly decoded, then with very high probability, there are some similar patches around it. Such a property of nonlocal image similarity motivates us to rank all the potential candidate blocks according to the minimum distance with the patches in a nonlocal search window. By including the texture direction and scale into the above minimization framework, we could further improve the error correcting performance, but we find that the additional gain is rather limited and the incurred complexity is large. The candidate (j) that gives the smallest (j) listen selected as the decoded block, Upon determining the index of the employed public key, the embedded message bits and the original image block can be straightforwardly recovered

Figure 3: Directly encrypted Lena of existing scheme

PROBLEM STATEMENT:

We say a data hiding method is lossless if the display of cover signal containing embedded data is same as that of original cover even though the cover data have been modified for data embedding. For example, the pixels with the most used color in a palette image are assigned to some unused color indices for carrying the additional data, and these indices are redirected to the most used color. This way, although the indices of these pixels are altered, the actual colors of the pixels are kept unchanged.

On the other hand, we say a data hiding method is reversible if the original cover content can be perfectly recovered from the cover version containing embedded data even though a slight distortion has been introduced in data embedding procedure. A number of mechanisms, such as difference expansion, histogram shift and lossless compression, have been employed to develop the reversible data hiding techniques for digital images. Recently, several good prediction approaches and optimal transition probability under payload-distortion criterion have been introduced to improve the performance of reversible data hiding.

III.PROPOSED METHOD

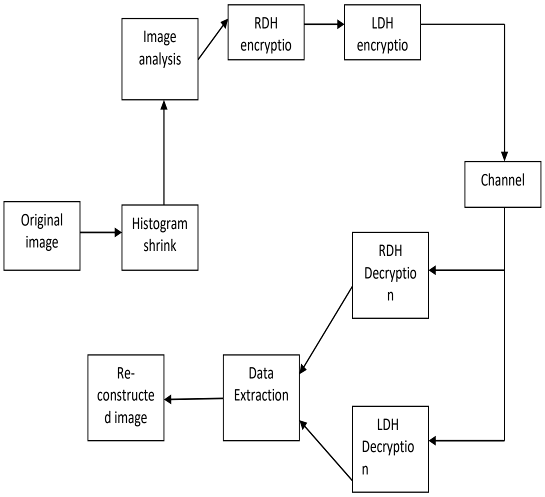

Fig 1: TWO LEVEL ENCRYPTION SYSTEM

In this method, we followed the workflow of a Reversible Data hiding (RDH) and Lossless Data hiding (LDH) scheme for encrypted images. The process includes three actors, the content owner encrypts the original image and sends it to the data hider; the data hider creates the marked image and sends to the receiver; and the receiver reconstruct the original image through decryption and data extraction. In fig. 1 the sketch of the complicated architecture is represented.

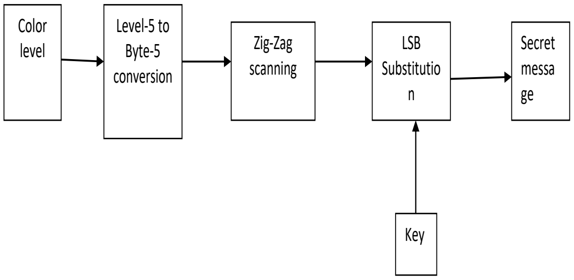

Fig 2: Reversable Data Hiding

The RDH process includes 4 sub processes and 4 different algorithms, namely encryption, embedding, decryption and recovery.

Encryption: Image encryption process can be defined as follows:

let the size of the input image is M×N, then it can be transformed into gray scale image by the following formula

I(i,j) = I gray(i,j) × (a + b)

Where, I = original image, 2a = M and 2b = N and Igray(i,j) = grayscale weight generated from the RGB scale. Now the encrypted image

IE(i,j) = I(i,j) ⊕ K(i,j)

Where K(i,j) is the key matrix generated using any asymmetric random function of order M × N.

Converting the three planes (Red, Green and Blue) of the stego image to one column of decimal pixels values using zigzag scanning (zigzag scanning for each plane). The size of the column vector will be (M×N×3) pixels, where (M) indicates to the number of rows in the original image, (N) indicates to the number of columns in the original image and (3) is the number of planes of the original image. Converting the column vector of pixels values to its representation in the binary value. After that, the size of the obtained matrix equal to (M×N×3×8) bits, where (8) indicates to the number of bits (where each pixel in the image is represented by one byte that equals to 8 bits).Then Data Embedding is performed through LSB substitution, Image marking or data embedding process can be defined as follows: The embedding operation is done only with some marked blocks of encrypted image. A series of operation are done between two consecutive pixel values to make some changes in the 3 LSB.

Thereafter a secret bit is embedded in the 4th LSB as marked embedded pixel. We have gone through a few reversible methods and used different combinations for data embedding. The adhered method is the best among them in terms of image recovery. Therefore, based on the reversibility constraint, we have chosen this proposed method. Here we divide the encrypted image IE into non overlapping image blocks of order Z × Z. Let it be n. For all alternatives block Bq starting from q=1 to n, i.e. for all even counting blocks, now embedding into a pixel can be made as follows:

a. Let the 1 st row be unchanged.
b. Perform the XOR operation between the three LSB bits of the consecutive rows x and y.
c. If the XOR result is 000, then the pixel will remain unchanged. Else Left rotate the 3 LSB of row x and flip the 4 th LSB. Continue step 2 for all marked blocks. Finally combine the blocks to form the embedded image.

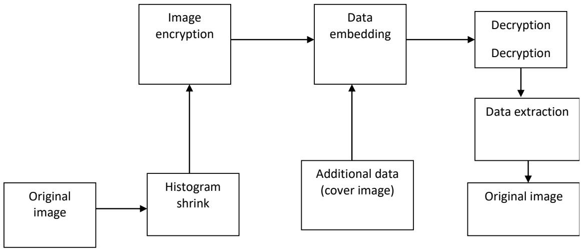

Fig 3: Lossless Data Hiding

Histogram is a statistical representation. The histogram of any digital image is a graphical representation of intensity distribution in an image. It represents the number of pixels for each intensity value. Distribution of intensity values in an image can be judged by looking at the histogram of the image. If I is a digital image with gray level range [0, Z − 1], the histogram of image I can be defined as a discrete function H(rk) such that: H(rk) = nk where, rk is defined as the k th gray level and nk is defined as the number of pixels having rk gray level.

Data embedding: The basic histogram bin shifting technique uses the histogram of original cover image. The main idea behind using the histogram is to utilize the peak point (the most frequently occurring pixel value) and zero point (the pixel value corresponding to which there is no gray scale value in the image) of the histogram of original image. The pixels between peak point and zero point has been shifted by 1 unit to create space next to peak point and watermark bits are embedded in this space. For this process, histogram of given image is generated. Peak point and zero point of the histogram are stored. It is assumed that the value of peak point is always less than the value of zero point. Whole image is scanned in a sequence and all pixels between peak point and zero point are shifted to right by 1 to create space for data embedding next to the peak point. Again scan the image and where pixel value is found to be equal to peak point, check the to-be-embedded watermark bit sequence. If it is "1", the grayscale pixel value is incremented by 1, otherwise pixel value remains unchanged.

Extraction Procedure: For extraction of watermark and recovery of original cover image, watermarked image is scanned and if pixel value is found to be 1 greater than peak point value, "1" is extracted as watermark bit. If pixel value is equal to the peak point value, "0" is extracted as watermark bit. In this way, watermark is extracted from the watermarked image. Whole image is scanned once again and all pixel values y, such that y ∈ (peak point, zero point], are subtracted by 1. In this way, original image can be recovered. If a pixel is found having grayscale value 95 (i.e. 96 − 1), "1" is extracted as watermark bit and if pixel value is found equal to 96, "0" is extracted as watermark bit. In this way, watermark is extracted. For recovering the original image, whole watermark image is scanned once again, and if pixel value y is found such that y ∈ [25, 96], the pixel value y is incremented by 1. In this way, original Lena image can be recovered.

IV.RESULTS AND DISCUSSIONS

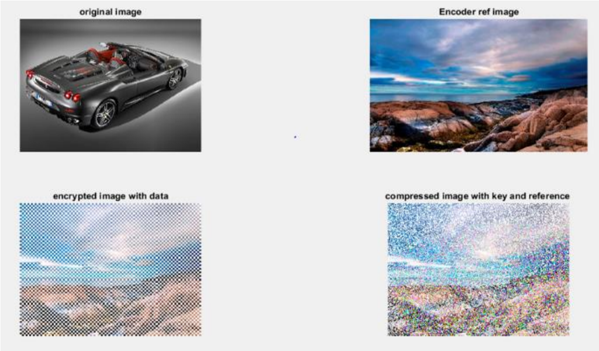
original image
Encoder ref image
encrypted image with data
compressed image with key and reference

Fig: 4- Two-Level Encryption

Fig: 5- Two-Level Decryption

Table 1: Summary of comparison

	EXISTING METHOD	PROPOSED METHOD
PSNR(dB)	21.50	40.0396
SSIM	0.239	0.523
MSE	23%	10%
BER	7%	4%
ENCRYPTION CAPACITY	45%	85%

V.CONCLUSION

In this paper, a novel reversible and lossless data hiding technique for encrypted images has been presented. it shows that the images recovered using proposed scheme are 100% accurate as compared to existing schemes in all the cases. Proposed scheme is also computationally faster than the existing schemes. Therefore, it can be concluded that the proposed scheme performs better as compared to existing schemes in the terms of the security and reversibility as well as computational time. This proves the effectiveness of the discussed scheme and thus, makes it suitable for privacy protection applications for sensitive fields.

REFERENCES

[1] Ahlfeldt; R.M., (2006) “Information Security in a Distributed Healthcare Domain”. Ph.D. thesis, University of Sk¨ovde, Department of Communication and Information

[2] Chandramouli R. and Memon N. (2001), "Analysis of LSB based Image Steganography Techniques", Proceedings of ICIP 2001, Thessaloniki, Greece, October 7−10.

[3] Deshpande N, Snehal K.,” Implementation of LSB Steganography and Its Evaluation for Various Bits” K.K.Wagh Institute of Engineering Education & Research, Nashik India

[4] http://www.appliedtrust.com/resources/security/every-company-needs-tohave-a-security -program

[5] Johnson, N.F. & Jajodia, S. (1998), “Exploring Steganography: Seeing the Unseen”, Computer Journal.

[6] Kekre H.B, Athawale A., Halarnkar P.N, (2009) “Performance Evaluation of Pixel Value Differencing and Kekre’s Modified Algorithm for Information Hiding in Images”, International Conference on Advances in Computing, Communication and Control, pp 342-346

[7] K Suresh Babu etal. (2005) “Authentication of secret information in image steganography”, Computer Journal

[8] Marvel L.M (1999) “Spread Spectrum Image Steganography,” IEEE transactions on image processing, vol. 8, no. 8, pp. 1075-1083.

[9] Moerland, T., “Steganography and Steganalysis”, Leiden Institute of Advanced Computing Science, www.liacs.nl/home/ tmoerl/privtech.pdf

[10] Mazurczyk W., Smolarczyk S., Szczypiorski K.:(2009) “Hiding Information in Retransmissions”, In: Computing Research Repository (CoRR), abs/0905.0363, arXiv.org E-print Archive, Cornell University, Ithaca, NY (USA).