RESEARCH ARTICLE OPEN ACCESS

Reversible Encrypytion and Information Concealment

Meenal V. Jagdale[1], Dr. Shubhalaxmi P. Hingway[2], Sheeja S. Suresh[3]
[1] P.G. student at Department of Electronics and Telecommunication G.H.Raisoni Institute of Engineering and Technology For Women . Nagpur –India
[2]Professor at Department of Electronics and Telecommunication G.H.Raisoni Institute of Engineering and Technology For Women . Nagpur –India
[3]Asst. Professor at Department of Electronics and Telecommunication G.H.Raisoni Institute of Engineering and Technology For Women . Nagpur –India

ABSTRACT
Recently, a lot of attention is paid to reversible data hiding (RDH) in encrypted pictures, since it maintains the wonderful property that the initial image cover will be losslessly recovered when embedded data is extracted, whereas protects the image content that is need to be kept confidential. Other techniques used antecedently are to embed data by reversibly vacating area from the pictures, that area unit been encryted, may cause some errors on information extraction or image restoration. In this paper, we propose a unique methodology by reserving room before secret writing (i.e reserving room before encryption) with a conventional RDH algorithmic rule, and thus it becomes straightforward for hider to reversibly embed data in the encrypted image. The projected methodology is able to implement real reversibility, that is, information extraction and image recovery area unit free of any error. This methodology embedds larger payloads for constant image quality than the antecedently used techniques, like for PSNR= 40db.

Keywords- Reversible data hiding, privacy protection, bar chart shift, image secret writing.

I. INTRODUCTION

Data concealment may be a technique that conceals secret knowledge into a carrier to convey messages. Digital pictures are one of all the media that's appropriate to convey messages due to many reasons. Firstly, digital pictures are typically transmitted over the internet which might raise very little suspicion. Secondly, the high correlation between pixels provides room for knowledge embedding. Once a digital image is employed as a carrier, the image accustomed introduce knowledge is thought because the cover image, and also the image with knowledge embedded is named the stego image. Within the embedding method, the pixels of the duvet image are changed and so, distortion happens. In general, the more the duvet image is distorted, the more vulnerable is that the stego image to steganalytic attempts. To forestall the stego image from being suspicious and detected, either visually statistically, the distortions caused by embedding the information ought to be as minimum as attainable, that imply that a prime quality embedded image is demanded. For many of the prevailing knowledge concealment techniques, the distortions caused by knowledge embedding are permanent i.e. the stego image cannot be rehabilitated to its original state. However, for a few applications, like medical or military pictures, it's desired that the first cover image are often utterly recovered owing to the wants for legal concerns or high exactness nature. To satisfy these needs, the reversible knowledge concealment theme for top quality pictures is introduced i.e reversible data hiding.

In 2003, Tian planned a reversible knowledge concealment technique using the distinction enlargement technique. In this technique, one bit is often embedded into 2 consecutive pixels; thus, the highest embedding capability is 0.5 bpp. Alattar generalized the distinction enlargement technique in order that n-1 bits are often embedded into n pixels, ensuring the highest embedding capability to be (n-1)/n bpp. However, the distinction enlargement based mostly reversible knowledge concealment strategies have to be compelled to double the variations between pixels; thus, a bigger distortion happens and will not be appropriate for applications wherever prime quality pictures are demanded. In 2006, Ni et al. planned a completely unique histogram-shifting reversible knowledge concealment technique. In Ni et al.'s method, pixel values are changed one gray scale value at the most and so, a prime quality stego image are often achieved.

However, the highest payload is restricted by the peak height of the image histogram; thus, the payload of this technique is comparatively low. Hwang et al.also planned a reversible knowledge concealment technique supported histogram-shifting and had higher embedding potency compared to Ni et al.'s work.

In 2007, Thodi and Rodriguez planned a totally different technique by increasing the prediction errors.As the result of the prediction error is

sometimes smaller than the distinction between 2 consecutive pixel values, the stego image quality obtained by this technique is healthier than that of Tian's technique. However, Thodi and Rodriguez's technique is additionally supported by expansion-embedding technique, a bigger distortion could occur; thus, their technique isn't appropriate for applications requiring prime quality pictures.

II. PLANNED TECHNIQUE

Vacating space from the encrypted pictures losslessly is comparatively troublesome and conjointly typically inefficient. Thus, we use a method to reverse the order of encoding and vacating space, i.e. reserving room before encryption at content owner facet, the RDH tasks in encrypted pictures would be a lot natural and also easier that leads North American country to the framework, "reserving space before encoding (RRBE)".As shown in Fig. 1(b), the content owner initially reserves enough space on original image and so converts the image into its encrypted version with the encoding key. The data embedding method in encrypted pictures is inherently reversible for the data hider, solely has to accommodate data into the spare space previously emptied out. The information extraction and image recovery is the image of the Framework VRAE where standard RDH algorithm is the ideal operator for reserving space before encryption and might be simply applied to Framework RRBE to offer higher performance as compared with techniques from Framework VRAE. This can be as a result of the new framework, where we follow the customary concept that initially losslessly compresses the redundant image content (e.g.by applying best RDH techniques) and encrypts it with reference to protect the privacy. Next, we have a tendency to elaborate a sensible technique supported the Framework "RRBE", that primarily consists of 4 stages: generation of encrypted image, information concealment in encrypted image, information extraction and image recovery.

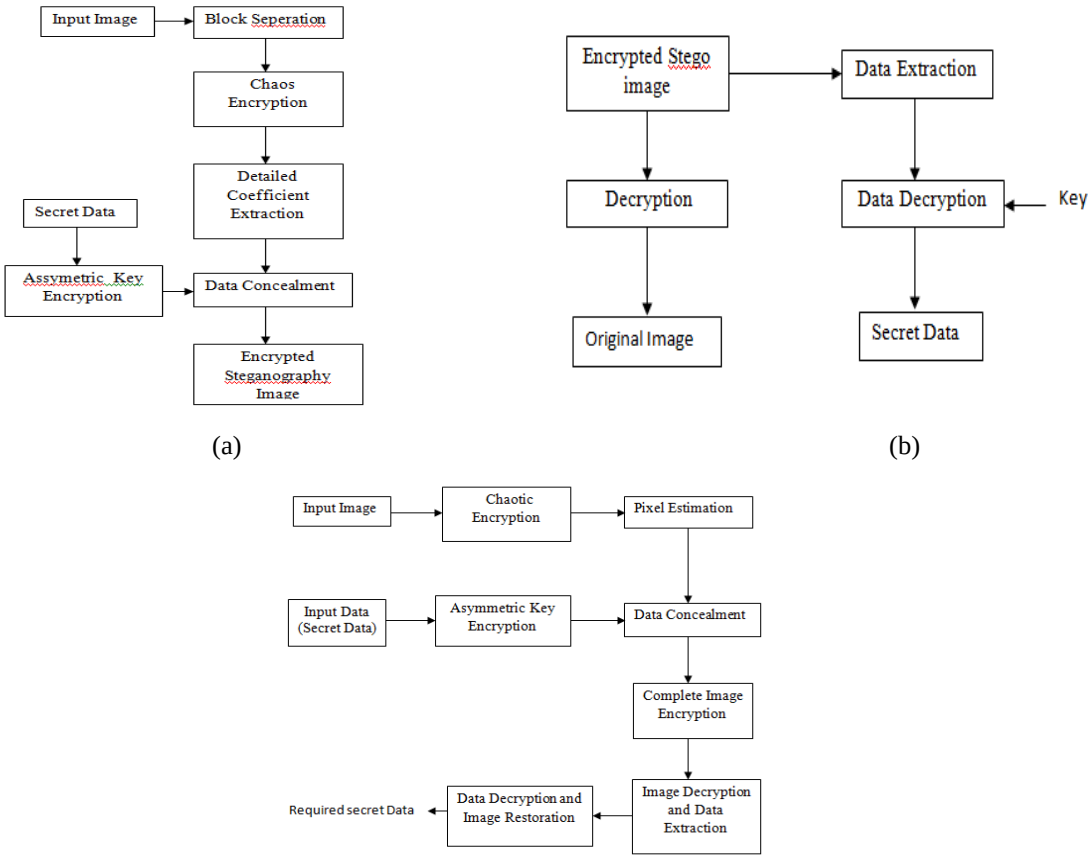


Fig 1. Block diagram: (a) Encryption and data embedding flow (b) Decryption (c) Complete architecture.

[A] GENERATION OF ENCRYPTED IMAGE

To construct the encrypted image 3 steps are followed: image partition, self-reversible embedding followed by image cryptography.

(1) Image Partition: The operator here for reserving room before encryption may be a customary RDH technique, therefore the goal of image partition is to construct a smoother space B, on that customary RDH algorithms are able to aquier higher performance .Assume the initial image C is of eight bits gray-scale image with its size M x N and pixels Cij € [0,255], 1≤ i ≤ M, 1≤ j ≤ N. First, the content owner extracts from the initial image, on the rows, several overlapping blocks whose variety is decided by the size of the embedded message, denoted by l. In detail, every block consists of rows, wherever m = [l/N] and therefore the variety of blocks may be computed through n = M – m + 1. For each block, here a function is stated to measure its first-order smoothness

$$f = \sum_{u=2}^{m} \sum_{v=2}^{N-1} \left| C_{u,v} - \frac{C_{u-1,v} + C_{u+1,v} + C_{u,v-1} + C_{u,v+1}}{4} \right| \quad \ldots.(1)$$

Higher f relates to blocks that contain comparatively additional complicated textures. The content owner, therefore, selects the actual block with the best f to be A, and puts it to the front of the image concatenated by the remainder half B with fewer rough-textured areas, as shown in Fig. 2.Here at the most 3 LSB-planes of A are used.

Fig (a) Original image

Fig (b) Final A

Fig(c) Final B

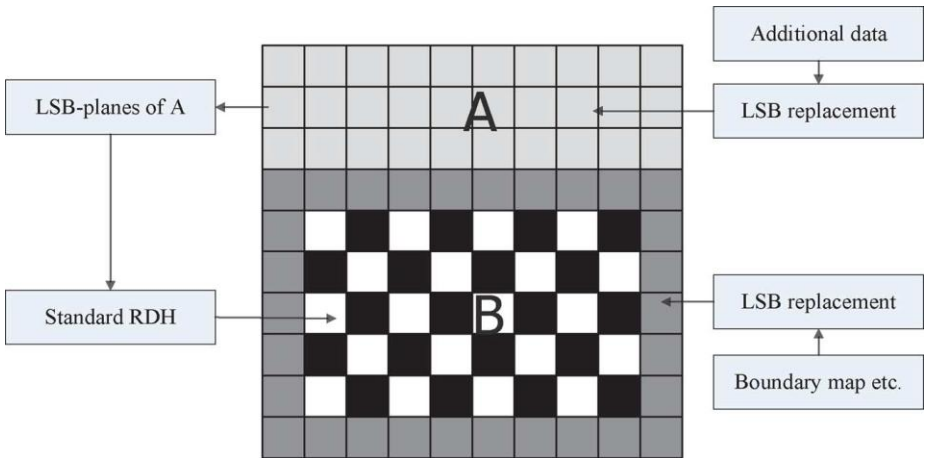


Fig 2. Illustration of Image patition and embedding process.

(2) Self-Reversible Embedding: The motive of self-reversible embedding is to embed the LSB-planes of A into B by using ancient RDH algorithms. Pixels in image B are firstly classified into 2 sets as, white pixels with its indices i and j satisfying (i +j)mod 2=0 and black pixels with indices (i +j)mod 2= 1 as in Fig. 2. Then, every white pixel Bi,j is calculable by the interpolation price obtained with the four black pixels encompassing it as follows,

$$\mathbf{B}'_{i,j} = w_1\mathbf{B}_{i-1,j} + w_2\mathbf{B}_{i+1,j} + w_3\mathbf{B}_{i,j-1} + w_4\mathbf{B}_{i,j+1},$$

….. (2)

Where the weight w_i $1 \leq i \leq 4$. Then the estimating error is calculated via eij = Bi,j – B'i,j alongside embedding some knowledge into the estimating error sequence with bar chart shift. After this we calculate the estimating errors of black pixels with the assistance of encompassing white pixels that are being changed. Then another estimating error sequence is made which will accommodate messages. Thus, we summarize that, to take advantage of all pixels of B, 2 estimating error sequences are created for embedding messages in each single-layer of embedding method. Using two-way bar chart shift, some messages are often embedded on every error sequence. In RDH algorithms, there happens the overflow and underflow once the natural boundary pixels modifies from 255 to 256 or from zero to -1. For its rejection, a boundary map is introduced to point whether or not boundary pixels in marked image natural or pseudo in extracting method.

(3) Image Cryptography: When the rearranged self-embedded image that is denoted by X is generated, we encrypt X to construct the encrypted image denoted by E .Using stream cipher, the encoding version of X are often simply obtained. For an example, a grey value Xi,j starting from 0 to 255 are often shown by 8 bits, Xi,j(0), Xi,j(1), . . . , Xi,j(7), such that

$$\mathbf{X}_{i,j}(k) = \left\lfloor \frac{\mathbf{X}_{i,j}}{2^k} \right\rfloor \bmod 2, \quad k = 0, 1, \ldots, 7.$$

….. (3)

The encrypted bits Ei,j(k) can be calculated through exclusive-or operation

$$\mathbf{E}_{i,j}(k) = \mathbf{X}_{i,j}(k) \oplus r_{i,j}(k),$$

….. (4)

Where ri,j(k) is generated via a regular stream cipher. Finally, embed 10 bits of data into LSB's of 1st 10 pixels in encrypted version of A to point knowledge hider the full range of rows and therefore the bit-planes he will enter information into.

[B] INFORMATION CONCEALMENT IN ENCRYPTED IMAGE

Once the information hider acquires the encrypted image E, he can embed some information into it, though he doesn't get access to the original image. The embedding method initiates by locating the encrypted version of A, denoted by AE. Since AE has been rearranged to the highest of E, it's simple for data hider to read 10 bits information in LSB's of 1st 10 encrypted pixels. After knowing the quantity of bit-planes and rows of pixels he can modify, the data hider merely adopts LSB replacement to substitute the offered bit-planes with extra data m Here, the data hider sets a label to signifies the top position of embedding method and then encrypts accordingly with the data concealment key to formulate marked encrypted image E'.

[C] INFORMATION EXTRACTION AND IMAGE RECOVERY

Extraction of information is totally freelance from image coding and therefore its order implies 2 completely different applications.

(1) Case 1: Extracting information From Encrypted Images:

In accordance to update and manage personal information of pictures that are encrypted for shielding clients' privacy, an inferior information manager might solely get access to the data concealment key and have to be compelled to manipulate data in encrypted domain. The order of information extraction before image coding guarantees the feasibleness. The information manager will decode the LSB-planes of AE and extract the extra information m by directly reading the decrypted version once supplied with the information concealment key.

(2) Case 2: Extracting information From Decrypted Images:

In the previous case each embedding and extraction of the information are manipulated in encrypted domain, whereas there exists a special scenario wherever the user desires to decode the image 1st and extract the information from the decrypted image once it's required.

(a) Generating the Marked Decrypted Image: To accumulate the marked decrypted image X" that is created of A" and B", the content owner ought to do following 2 steps:

• Step 1: With the cryptography key, the content owner decrypts the image except the LSB-planes of AE. The decrypted version of E' containing the embedded information are often calculated by,

$$\mathbf{X}''_{i,j}(k) = \mathbf{E}'_{i,j}(k) \oplus r_{i,j}(k) \quad \text{..... (5)}$$

And

$$\mathbf{X}''_{i,j} = \sum_{k=0}^{7} \mathbf{X}''_{i,j}(k) \times 2^k, \quad \text{..... (6)}$$

Where E'i,j(k) and X"i,j(k) area unit the binary bits of E'i.j and X"i,j obtained via (3) severally.

• Step 2: Rearrange A" and B" to its original state, we can acquire the plain image containing embedded information because the marked decrypted image X" is clone of rearranged X except LSB-planes of A. At the meanwhile, it keeps sensory activity transparency compared with original image C. More specifically, the distortion is introduced via 2 separate ways: the embedding method by modifying the LSB-planes of A and self-reversible embedding method by embedding LSB-planes of A into B.

(b) Information Extraction and Image Restoration: Nextly, the content owner will extract the information and recover original image after generating the marked decrypted image. The method is comparable to the normal RDH ways. The subsequent outlines the particular steps:

• Step 1: Record and decode the LSB-planes of A" consistent with the information concealment key; extract the information till the top label is reached.

• Step 2: Extract LN, RN, LM, RM, LP, RP, Rb, x and boundary map from the LSB of marginal space of B". Then, scan B" to undertake the subsequent steps.

• Step 3: If R_b is equal to zero, which implies no black pixels participate in embedding method, move to Step5.

• Step 4: Calculate estimating errors e'i,j of the black pixels B"i,j . If B"i,j belongs to [1, 254], recover the estimating error and original pixel value in a very reverse order and extract embedded bits once e'i,j is equal to LN, LM (or LP), RM (or RP) and RN. If b = 0, skip this, else operate like B"i,j € [1, 254] . Repeat this step till the part of payload R_b is extracted.

• Step 5: Calculate estimating errors e'i,j of the white pixels B"i,j ,and extract embedded bits and recover white pixels within the same manner as with Step 4.

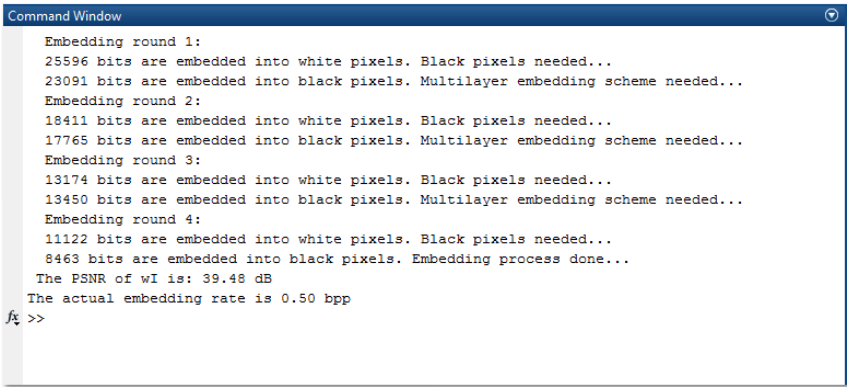
• Step 6: Continue Step 2 to Step 5, (x – 1) rounds on B" and merge all extracted bits to create LSB-planes of A. Until now, we've utterly recovered B.

• Step 7: Replace marked LSB-planes of A" with its original bits extracted from B" to urge original cover image C.

OUTPUT OBTAINED:

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

Fig 3.(a) Original image, (b) encrypted image, (c) decrypted image containing message, (d) recovery version.



(e) Corresponding command window indicating the increased PSNR value to 39.48db.

III .CONCLUSION

Reversible information concealment in encrypted pictures is a new idea drawing attention owing to the privacy-preserving needs from cloud information management. In previous strategies RDH method was incorporated in encrypted pictures by vacating space once encrypting the image, while in opposition with it we implemented reserving room before encrypting the image. Hence, the information hider have an advantage of the additional area emptied in the previous stage and make the information concealment method relatively more easy and effortless. This technique profits over all the ancient RDH techniques for plain pictures and reach high performance with no loss of secrecy. Moreover, this novel technique gains separate information extraction, real reversibility and great improvement on the standard of marked decrypted pictures.

REFERENCES

[1] Kede Ma,Weiming Zhang,Xeianfeng Zhao,"*Reversible data hiding in encrypted images by reserving room before encryption*" IEEE Trans. On information forensic and security,VOL.8NO.3 March 2013.

[2] W. Zhang, B. Chen, and N. Yu, "*Improving various reversible data hiding schemes via optimal codes for binary covers*," *IEEE Trans.Image Process.*, vol. 21, no. 6, pp. 2991–3003,Jun. 2012.

[3] W.Zhang, B. Chen, and N. Yu, "*Capacity-approaching codes for reversible data hiding*," in *Proc 13th Information Hiding (IH'2011) LNCS 6958*, 2011, pp. 255–269, SpringerVerlag.

[4] T. 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.

[5] X. L. Li, B. Yang, and T. Y. Zeng, "*Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection*, *IEEE Trans. Image Process.*, vol. 20, no. 12, pp. 3524–3533, Dec. 2011.

[6] L. Luo *et al.*, "*Reversible image watermarking using interpolation technique*," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 1, pp. 187–193,Mar. 2010.

[7] P. Tsai, Y. C. Hu, and H. L. Yeh, "*Reversible image hiding scheme using predictive coding and histogram shifting*," *Signal Process.*, vol.89, pp. 1129–1143, 2009.

[8] D.M. Thodi and J. J. Rodriguez, "*Expansion embedding techniques for reversible watermarking,*" *IEEE Trans. Image Process.*, vol. 16, no. 3, pp. 721–730, Mar. 2007.

[9] Z. Ni, Y. Shi, N. Ansari, and S. Wei, "*Reversible data hiding*," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 16, no. 3, pp. 354–362, Mar.2006.

[10] J. Tian, "*Reversible data embedding using a difference expansion*," *IEEE Trans. Circuits Syst.Video Technol.*, vol. 13, no. 8, pp. 890–896 Aug. 2003.

[11] J. Fridrich and M. Goljan, "*Lossless data embedding for all image formats*," in *Proc. SPIE Proc. Photonics West, Electronic Imaging, Securityand Watermarking of Multimedia Contents*, San Jose, CA, USA, Jan. 2002, vol. 4675, pp. 5