Journal of Engineering Sciences
Vol 11, Issue 10, OCT/2020
ISSN NO:0377-9254

A Reversible Data Hiding Based Cryptography for Effective Image Encryption

[1]Dr.Chinmaya Kumar Pradhan, [2]Atchala Bhaskar Reddy
[1]*Assoc. Professor, Dept.of ECE, Chalapathi Inst of Engineering & Technology,Lam,Guntur,AP,India*
[2]*(PG Student),Dept.of ECE, Chalapathi Inst of Engineering & Technology,Lam,Guntur,AP,India.*

Abstract:
In reversible data hiding techniques, the values of host data are modified according to some particular rules and the original host content can be perfectly restored after extraction of the hidden data on receiver side. In this paper, the optimal rule of value modification under a payload- distortion criterion is found by using an iterative procedure, and a practical reversible data hiding scheme is proposed. The secret data, as well as the auxiliary information used for content recovery, are carried by the differences between the original pixel-values and the corresponding values estimated from the neighbours. Here, the estimation errors are modified according to the optimal value transfer rule. Also, the host image is divided into a number of pixel subsets and the auxiliary information of a subset is always embedded into the estimation errors in the next subset. A receiver can successfully extract the embedded secret data and recover the original content in the subsets with an inverse order. This way, a good reversible data hiding performance is achieved.

Key Words: Distortion, Payload, Reversible Data Hiding (RDH) Estimation Errors, Data Encryption, Accuracy & etc.

I. INTRODUCTION

Data hiding technique aims to embed some secret information into a carrier signal by altering the insignificant components for copyright protection or covert communication. In general cases, the data-hiding operation will result in distortion in the host signal. However, such distortion, no matter how small it is, is unacceptable to some applications, e.g., military or medical images. In this case it is imperative to embed the additional secret message with a reversible manner so that the original contents can be perfectly restored after extraction of the hidden data. A number of reversible data hiding techniques have been proposed, and they can be roughly classified into three types: lossless compression based methods, difference expansion (DE) methods, and histogram modification (HM) methods. The lossless compression based methods make use of statistical redundancy of the host media by performing lossless compression in order to create a spare space to accommodate additional secret data. In the RS method [1], for example, a regular-singular status is defined for each group of pixels according to a flipping operation and a discrimination function. The entirety of RS status is then

losslessly compressed to provide a space for data hiding. Alternatively, the least significant digits of pixel values in an L-ary system [2] or the least significant bits (LSB) of quantized DCT coefficients in a JPEG image [3] can also be used to provide the required data space. In these reversible data hiding methods, a spare place can always be made available to accommodate secret data as long as the chosen item is compressible, but the capacities are not very high.

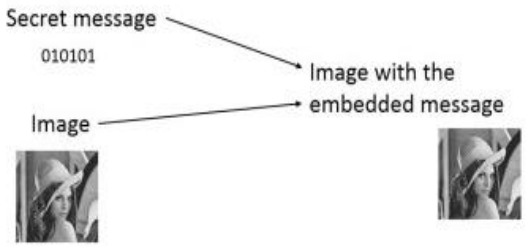

Figure 1: The Basic Procedure for Data Embedded into Images.

In the difference expansion method, differences between two adjacent pixels are doubled so that a new LSB plane without carrying any information of the original is generated. The hidden message together with a compressed location map derived from the property of each pixel pair, but not the host information itself, is embedded into the generated LSB plane. Since compression rate of the location map is high, and almost each pixel pair can carry one bit, the DE algorithm can embed a fairly large amount of secret data into a host image. Furthermore, various techniques have been introduced into DE algorithm to improve its performance, including generalized integer transform , pixel value prediction mechanism, histogram shifting operation, prediction of location map, simplification of location map and improvement of compressibility of location map.

Also, these application requires lossless recovery of the original image and hence the need of reversibility. The system proposes a framework of Camouflage of Image by Reversible Image Transformation (RIT). RIT-based RDH-EI shifts the semantic of the original image to the semantic of another image and thus protects the privacy of the original image and reversibility means that they can be loselessly restored from the transformed image. Therefore RIT can be viewed as a special encryption scheme, called “Semantic Transfer Encryption (STE)”.Because the camouflage image is in a form of plaintext, it will avoid the notation of the cloud server, and the cloud server can easily embed additional data into the camouflage image with traditional RDH methods for plaintext images. Encryption and data hiding are two effective means of data protection. While the encryption techniques convert plaintext content into unreadable ciphertext, the data hiding techniques embed additional data into cover media by introducing slight modifications. There are a number of schemes which performs data hiding and encryption jointly. Different methods are used to data hide. But sometimes data hiding in images causes damages to the original image and also to the embedded data during extraction. It is feasible in the applications like cloud storage and medical systems. Now a day’s outsourcing data to the cloud became more popular service .This cloud storage is mainly used to store videos or images which needs large storage area. The cloud storage may embed some additional data to the images such as owner name or image

category etc. to manage the outsourced data. But the cloud storage has no authority to damage the user data. So reversible or lossless data hiding can be used for data hiding. Also It is vital to protect the privacy of data. Under such demands, reversible data hiding in encrypted images (RDH-EI) got more attraction.

II. LITERATURE REVIEW

There are many are techniques available regarding reversible data hiding in encrypted image such as follows.

2.1 Secret Fragment Visible Mosaic Images to Information Hiding

Lai et al. [3] proposes an image transformation technique, which selects a target image similar to the secret image, then replaces each block of the target image by a similar block of the secret image and embeds the map between secret blocks and target blocks; it forms an Encrypted image of the secret image. A greedy search method is used to find the most similar block. Although Lai et al.'s method is reversible, it is only suitable for a target image similar with the secret image, and the visual quality of encrypted image is not so good.

2.2 Via Secret Fragment Visible Mosaic Images by Nearly

Reversible Color Transformations Lee et al. [4] improve Lai et al.'s method by transforming the secret image to a randomly selected target image without any use of database. In Lee et al.'s method, each block of the secret image is transformed to a block of the target image with a reversible color transformation [5], and then the required information for restoring secret image, such as parameters, indexes of block, is added into the transformed blocks, it gives Encrypted image. Lee et al.'s method can transform a secret image to a randomly selected target image, and increase quality of the encrypted image. However, in Lee et al.'s method, the transformation is not reversible. So that secret image cannot be losslessly reconstructed.

2.3 By Reserving Room before Encryption

Authors [6] proposed a novel method for RDH in encrypted images, for that method they do not "vacate room after encryption" as done previously but "reserve room before encryption with a traditional RDH algorithm, and thus it is easy for the data hider to reversibly embed data in the encrypted image. The proposed method can achieve real reversibility that is data extraction and image recoveries are error free. First up all they empty out room by embedding LSBs of some pixels into other pixels with a traditional RDH method and then encrypt the image, so the positions of these LSBs in the encrypted image can be used to embed data. Not only the proposed method separate data extraction from image decryption but also achieves excellent performance.

2.4 With Public Key Cryptography

This correspondence [7] proposed a lossless, reversible and data hiding schemes for public-key-encrypted images probabilistic and homomorphic properties of cryptosystems. With these schemes, the pixel

division/reorganization is avoided and the encryption/decryption is performed on the cover pixels directly so that the amount of encrypted data and the computational complexity are lowered. Due to data embedding on encrypted domain may result in a little bit distortion in plaintext domain due to the homomorphic property, the embedded data can be extracted and the original content can be recovered from the directly decrypted image. With the combined technique, a receiver may extract a part of embedded data before decryption, and extract another part of embedded data and recover the original plaintext image after decryption.

2.5 Via Key Modulation

The data embedding is achieved through a public key modulation [8] mechanism, which allows us to embed the data via simple XOR operations, without accessing the secret encryption key. At the decoder side, a powerful two-class SVM classifier is designed to distinguish encrypted and non encrypted image patches, allowing us to jointly decode the embedded message and the original image signal. The proposed approach provides higher embedding capacity and is able to perfectly reconstruct the original image as well as the embedded message.

2.6 With Distributed Source Encoding

This technique [9] aims to enhance scheme of reversible data hiding (RDH) in encrypted images using Slepian-Wolf source encoding which was inspired by DSC? After the original image is encrypted by the content owner using a stream cipher, the data-hider compresses a series of selected bits taken from the encrypted image to make spare room to accommodate for the secret data. With two different keys, the proposed method is separable. The hidden data can be completely extracted using the embedding key, and the original image can be approximately reconstructed with high quality using the encryption key. If the receiver has both the embedding and encryption keys, receiver can extract the secret data and perfectly recover the original image. The proposed method achieves a high embedding payload and good image reconstruction quality and avoids the operations of room-reserving by the sender.

2.7 By Patch-level Sparse Representation

In [10] proposed a novel method called the HC_SRDHEI, which inherits the merits of RRBE, and the separability property of RDH methods in encrypted images for a better relation between neighbor pixels, we propose consider the patch-level sparse representation when hiding the secret data. Compared to state-of-the-art alternatives, the room vacated for data hiding. The data hider simply adopts the pixel replacement to substitute the available room with additional secret data. The data extraction and cover image recovery are separable, and are free of any error. Experimental results on three datasets shows that the proposed method has average MER can reach 1.7 times as large as the previous best alternative method provides. The performance analysis implies that proposed method has a very good potential for practical applications.

2.8 Using Side Match

W. Hong [11] proposed an improved version of Zhang's reversible data hiding method in encrypted images. Which divides the encrypted image into blocks, and each block carries one bit by flipping three LSBs of a set of pre-defined pixels. The data extraction and image recovery can be achieved by examining the block smoothness. Data recovery of block is performed in descending order of the absolute smoothness difference between two candidate blocks. The side match technique is employed to further reduce the error rate.

2.9 Encrypted Image based on Chaotic Map

A reversible data hiding technique in encrypted images based on chaotic maps [12] in which the secret data is embedded into the encrypted image and the original cover image can be losslessly recovered at the receiver end. Chaos based cryptosystems are being widely used for practical applications due to their properties like pseudo randomness, sensitivity on initial conditions and system parameters and the combination of reduced execution time, high security and high complexity to break the cryptosystem. This proposed system provides improved retrieved cover image quality, High data hiding capacity, Data extraction without error and a Lower bound PSNR of 50.91dB it gives better results than the existing system.

2.10 Resolution Progressive Compression Scheme

Wei Liu et al. [13] in this proposal, resolution progressive compression scheme is used which compresses an encrypted image progressively in resolution, such that the decoder can observe a low resolution version of the image, study local statistics based on it, and use the statistics to decode the next resolution level. The encoder starts by sending a down sampled version of the cipher text. At the decoder, the corresponding low-resolution image is decoded and decrypted, from which a higher-resolution image is obtained by intra-frame prediction. The predicted image, together with the secret encryption key, is used as the side information (SI) to decode the next resolution level. This process is iterated until the whole image is decoded. So this multi-resolution approach makes it possible to have access to part of the spatial source data to generate more reliable spatial and temporal side information. But there is need to increase the efficiency of overall data compression to avoid the loss of any kind of data.

2.11 Analysis of the Local Standard Deviation of the Marked Encrypted Images

W. Puech et al. [14] proposed an analysis of the local standard deviation of the marked encrypted images in order to remove the embedded data during the decryption step for protection of multimedia based on Encryption and watermarking algorithms rely on the Kirchhoff's principle, all the details of the algorithm are known, and only the key to encrypt and decrypt the data should be secret. The first one is when there is homogeneous zones all blocks in these zones are encrypted in the same manner. The second problem is that block encryption methods are not robust to noise. Indeed, because of the large size of the blocks the encryption algorithms per block, symmetric or asymmetric cannot be robust to

noise. The third problem is data integrity. The combination of encryption and data-hiding can solve these types of problems hence by using this approach a reversible data hiding method for encrypted images is able to embed data in encrypted images and then to decrypt the image and to rebuild the original image by removing the hidden data but it is not possible to use when high capacity reversible data hiding method for encrypted images.

2.12 Chaos Security

Christophe Guyeux et al. [15] developed a new framework for information hiding security, called chaos security. In this work, the links among the two notions of security is deepened and the usability of chaos-security is clarified, by presenting a novel data hiding scheme that is twice stego and chaos-secure. The aim of this approach is to prove that this algorithm is stego-secure and chaos-secure, to study its qualitative and quantitative properties of unpredictability, and then to compare it with Natural Watermarking. Some of the probabilistic models are used to classify the security of data hiding algorithms (Runge-Kutta algorithm) in the Watermark Only Attack (WOA) framework. Hence method possesses the qualitative property of topological mixing, which is useful to withstand attacks but cannot be applied in KOA and KMA (Known Message Attack) setup due to its lack of expansively schemes which are expansive.

2.13 Distributed Source-Coding Principles

Mark Johnson et al. [16] proposed the novelty of reversing the order of these steps, i.e., first encrypting and then compressing, without compromising either the compression efficiency or the information-theoretic security. In this method first data encryption is used and then the encrypted source is compressed but the compressor does not have access to the cryptographic key, so it must be able to compress the encrypted data without any knowledge of the original source. At first glance, it appears that only a minimal compression gain, if any, can be achieved, since the output of an encrypt or will look very random. However, at the receiver, there is a decoder in which both decompression and decryption are performed in a joint step. In a broad spectrum in this approach, the encrypted data can be compressed using distributed source-coding principles as the key will be available at the decoder but in some cases the possibility of first encrypting a data stream and then compressing where compressor does not have knowledge of the encryption key. Among from all these works we observed following disadvantages

- Not having high capacity to encrypt more data.
- Limited Decryption is possible only.
- Payload of this method is low since each block can only carry one bit.

III. PROPOSED METHODOLOGY

Reversible data hiding is a technique to embed additional message into some distortion-unacceptable cover media, such as military or medical images, with a reversible manner so that the original cover content can be perfectly restored. The Proposed System Block diagram is shown in the connection diagram in Figure 2.

A number of reversible data hiding methods have been proposed in recent years. In difference expansion method [5], differences between two adjacent pixels are doubled to generate a new least significant bit (LSB) plane for accommodating additional data.

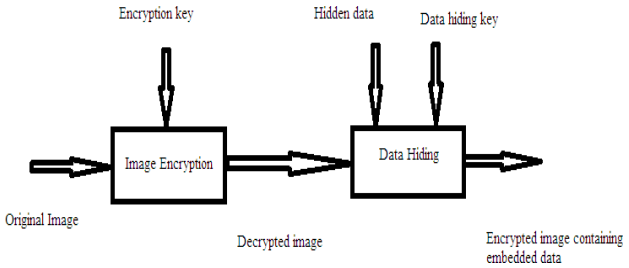

Figure 2: Data hiding in Encrypted image.

A data hider can also perform reversible data hiding using a histogram shift mechanism [8], which utilizes the zero and peak points of the histogram of an image and slightly modifies the pixel gray values to embed data into the image. Another kind of method makes use of redundancy in a cover by performing lossless compression to create a spare space for data embedding [3]. Furthermore, various skills have been introduced into the typical reversible data hiding approaches to improve the performance. the proposed scheme, the secret data, as well as the auxiliary information used for content recovery, are carried by the differences between the original pixel-values and the corresponding values estimated from the neighbours, and the estimation errors are modified according to the optimal value transfer matrix. The optimal value transfer matrix is produced for maximizing the amount of secret data, i.e., the pure payload, by the iterative procedure described in the previous section. That implies the size of auxiliary information does not affect the optimality of the transfer matrix. By dividing the pixels in host image into two sets and a number of subsets, the data embedding is orderly performed in the subsets, and then the auxiliary information of a subset is always generated and embedded into the estimation errors in the next subset.

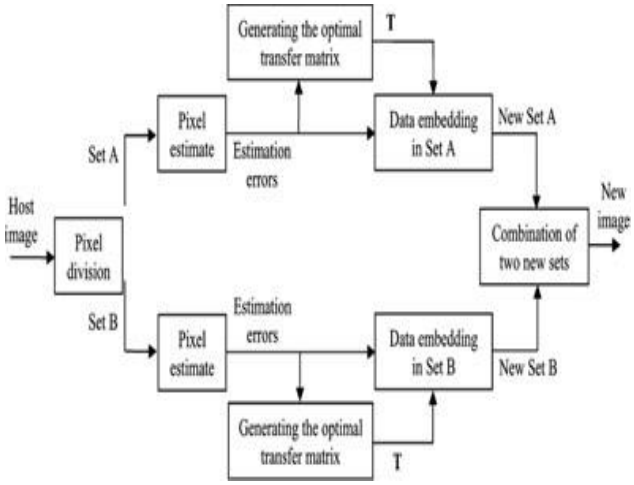

Figure 3: Proposed Methodology Block Diagram.

This way, a receiver can successfully extract the embedded secret data and recover the original content in the subsets with an inverse order.

3.1 Data Embedding

The data embedding procedure is sketched in Fig. 3. Denote the host pixels as P u,v where u and v are indices of row and column, and divide all pixels into two sets: Set A containing pixels with even (u+v) and Set B containing

other pixels with odd(u+v) . Fig. 3 shows the chessboard- like division. Clearly, the four neighbors of a pixel must belong to the different set. For each pixel, we may use four neighbors to estimate its value,

$$e_{u,v} = p_{u,v} - p^{(E)}{}_{u,v}.$$

That means the pixels in Set A/B are estimated by using the pixels in B/A. The data embedding procedure is made up of two parts: data embedding in estimation errors of Set A, and data-embedding in estimation errors of Set B. Before data embedding in estimation errors of Set A, we first find the optimal weights with the least square error,

$$\{w^*_{-1,0}, w^*_{1,0}, w^*_{0,-1}, w^*_{0,1}\} = \underset{\{w_{-1,0}, w_{1,0}, w_{0,-1}, w_{0,1}\}}{\arg\min} \sum_{p_{u,v} \in \text{Set } A} e^2_{u,v}.$$

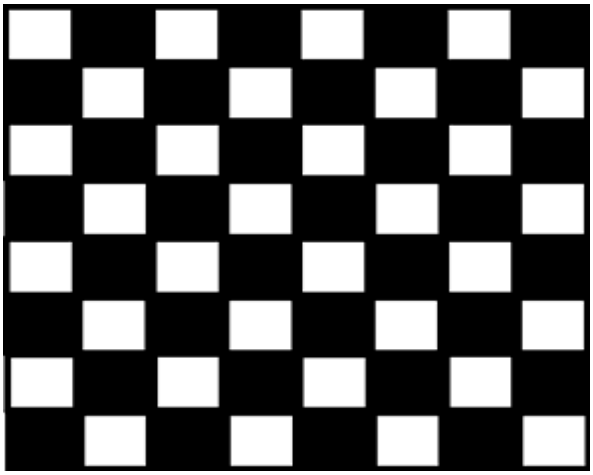

Figure 4: Pixel division in chessboard fashion. The white and black pixels belong to Sets A and B respectively.

That means the pixels in Set A/B are estimated by using the pixels in B/A. The data embedding procedure is made up of two parts: data-embedding in estimation errors of Set A, and data-embedding in estimation errors of Set B. Before data embedding in estimation errors of Set A, we first find the optimal weights with the least square error,

$$p^{(E)}{}_{u,v} = w_{-1,0} \cdot p_{u-1,v} + w_{1,0} \cdot p_{u+1,v} + w_{0,-1} \cdot p_{u,v-1} + w_{0,1} \cdot p_{u,v+1},$$

3.2 Data Extraction and Content Recovery

When having an image containing embedded data, the receiver firstly divides the image into Sets A and B, and divides Sets A and B into a number of subsets using the same manner. Then, extract and AI from the LSB of the last subset in Set B, and decompose as the weight values, the histogram difference of the first subsets and the number of iterations. With the weight values, the receiver can obtain the estimation error of each pixel in the first subsets, and with the histogram difference and the iteration number, he can use the histogram difference to retrieve the original scaled histogram and implement the iterative procedure to retrieve the optimal transfer matrix used for data- embedding in the first subsets. Then, the receiver recovers the original content and extracts the hidden data in Subset of Set B. Since the first part of AI contains the labels of saturated pixels and the original values of the first type of saturated pixels, the first type of saturated pixels in Subset can be localized and their original values can be recovered. For the second types of saturated pixels and the unsaturated pixels, after calculating the probability, the receiver can convert the second part of AI into a sequence of original estimation error by arithmetic decoding. Thus, the original pixel

values are recovered as where and are the pixel value and estimation error in received image, and is the original estimation error. Furthermore, with the original estimation errors and the new estimation errors, after calculating the probability, the receiver can also retrieve the embedded data by arithmetic decoding. This way, the auxiliary information extracted from a subset is used to recover the original content of the previous subset, and then the embedded data in the previous subset are extracted by using the recovered original estimation error. That means the original content and the hidden data in the subsets of Set B, except the last one, can be recovered and extracted with an inverse order. Then, the receiver can decompose the payload hidden in the subsets into AI of Set A, , LSB of Subset of Set B, and the embedded secret data. While the LSB of Subset of Set B is used to recover the original content of the subset, is used to retrieve the optimal transfer matrix and the estimation error of each pixel in Set A. Similarly, the original content and the hidden data in the subsets of Set A can be also recovered and extracted with an inverse order. At last, by concatenating the secret data hidden in Sets A and B, the receiver reconstructs the entire secret data.

IV. RESULTS & DISCUSSION

Four images, Lena, Baboon, Plane and Lake, all sized 512 x 512, shown in Fig. 4 were used as the host images. Both Set A and Set B were divided into 16 subsets. Since the auxiliary information of a subset is generated after data embedding and embedded into the next subset, we should ensure the capacity of a subset is more than the data amount of auxiliary information of the previous subset. This way, a receiver can successfully extract the embedded secret data and recover the original content in the subsets with an inverse order. On the other hand, the optimal transfer mechanism implemented in every subset except the last one is used to achieve a good payload-distortion performance.

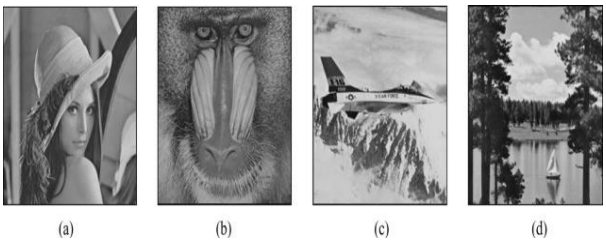

Figure 5: Host images: (a) Lena, (b) Baboon, (c) Plane, and (d) Lake.

Figure 6: Two versions of Lena containing the embedded secret data.

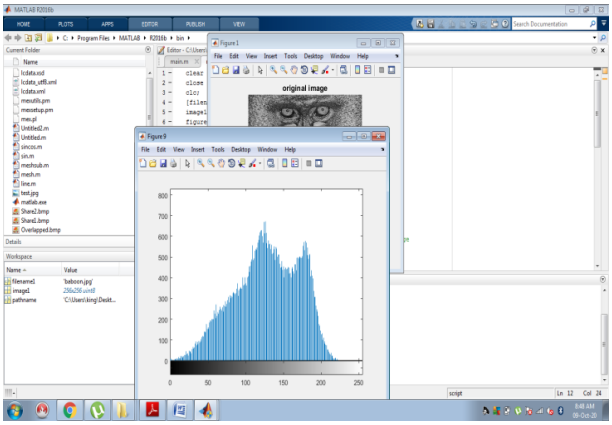

Fig 7: Image Histogram.

Journal of Engineering Sciences
Vol 11, Issue 10, OCT/2020
ISSN NO:0377-9254

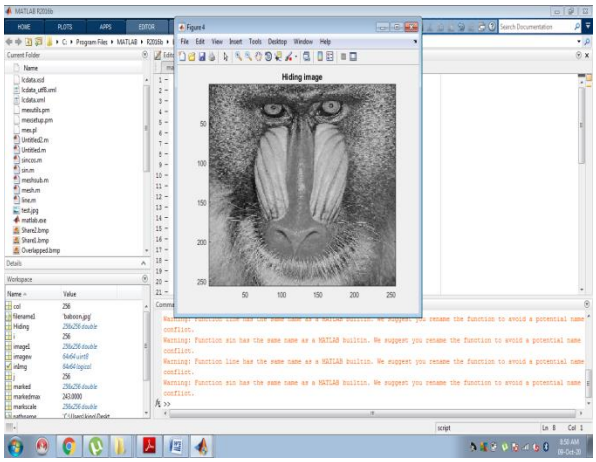

Fig 8: Data Encrypted Image.

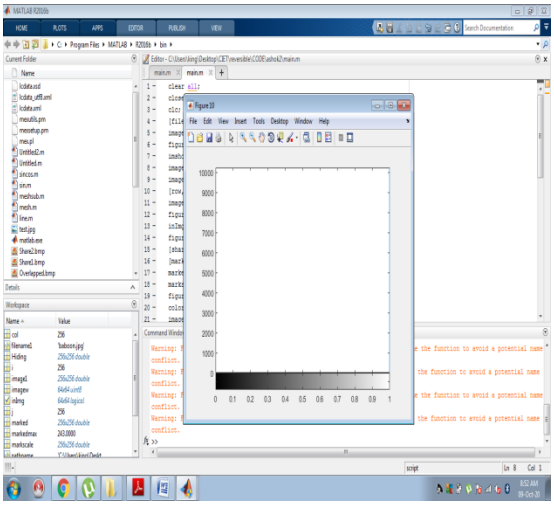

Fig 11: Overlapped Set 1& 2 Image.

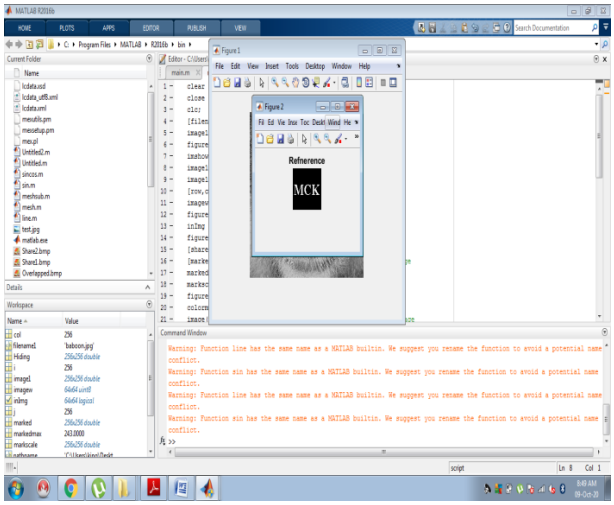

Figure 9: Reference Image.

For the last subset, a LSB replacement method is employed to embed the auxiliary information of the second last subset and for content recovery with an inverse order. So, we hope the size of the last subset is small. Considering the two aspects, we make the subset sizes identical and let . In this case, the last subset occupies only 1/32 of cover data and almost does not affect the payload-distortion performance. Fig. 5 gives two versions of Lena with different amounts of embedded secret data. Actually, the iteration number for producing the

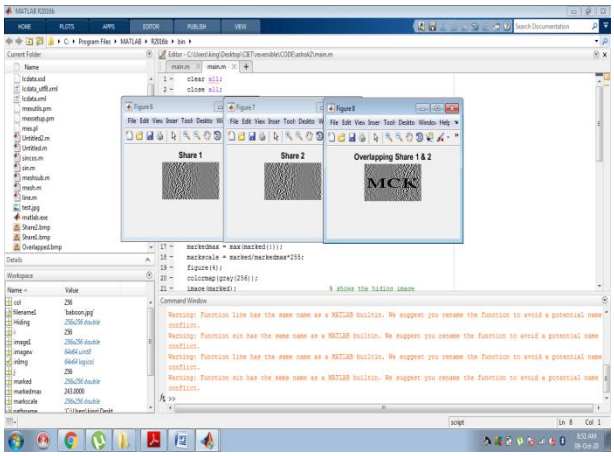

Fig 10: Overlapping Set 1& 2 Image.

V.CONCLUSION

In order to achieve a good payload-distortion performance of reversible data hiding, this work first finds the optimal value transfer matrix by maximizing a target function of pure payload with an iterative procedure, and then proposes a practical reversible data hiding scheme. The differences between the original pixel-values and the corresponding values estimated from the neighbors are used to carry the payload that is made up of the actual secret

data to be embedded and the auxiliary information for original content recovery. According to the optimal value transfer matrix, the auxiliary information is generated and the estimation errors are modified. Also, the host image is divided into a number of subsets and the auxiliary information of a subset is always embedded into the estimation errors in the next subset. This way, one can successfully extract the embedded secret data and recover the original content in the subsets with an inverse order. The payload-distortion performance of the proposed scheme is excellent. For the smooth host images, the proposed scheme significantly outperforms the previous reversible data hiding methods. The optimal transfer mechanism proposed in this work is independent from the generation of available cover values. In other words, the optimal transfer mechanism gives a new rule of value modification and can be used on various cover values. If a smarter prediction method is exploited to make the estimation errors closer to zero, a better performance can be achieved, but the computation complexity due to the prediction will be higher. The combination of the optimal transfer mechanism and other kinds of available cover data deserves further investigation in the future.

VI. REFERENCES

[1] I.-J. Lai and W.-H. Tsai, "Secret-fragment-visible mosaic image–a new computer art and its application to information hiding," IEEE Trans. Information Forensics and Security, vol. 6, no. 3, pp. 936–945, 2011.

[2] Y.-L. Lee and W.-H. Tsai, "A new secure image transmission technique via secret-fragment-visible mosaic images by nearly reversible color transformations," IEEE Trans. Circuits Syst. & Video Technol., vol. 24, no. 4, pp. 695–703, 2014.

[3] E. Reinhard, M. Ashikhmin, B. Gooch, and P. Shirley, "Color transfer between images," IEEE Computer Graphics and Applications, vol. 21, no. 5, pp. 34–41, 2001.

[4] K. Ma, W. Zhang, X. Zhao, N. Yu, F. Li, "Reversible data hiding in encrypted images by reserving room before encryption," IEEE Trans. on Information Forensics and Security, vol. 8, no. 3, pp. 553-562, Mar. 2013.

[5] Xinpeng Zhang, Jing Long, Zichi Wang, and Hang Cheng, "Lossless and Reversible Data Hiding in Encrypted Images with Public Key Cryptography,"IEEE Trans. on Circuits and Systems for Video Technology, 2015.

[6] J. Zhou, W. Sun, L. Dong, et al., "Secure reversible image data hiding over encrypted domain via key modulation," IEEE Trans. on Circuits and Systems for Video Technology, vol. 26, no. 3, pp. 441-452, Mar. 2016.

[7] Z. Qian, and X. Zhang, "Reversible data hiding in encrypted image with distributed source encoding," IEEE Trans. on Circuits and Systems for Video
Technology, vol. 26, no. 4, pp. 636-646, Apr. 2016.

[8]X. Cao, L. Du, X. Wei, et al., "High capacity reversible data hiding in encrypted images by patch-level sparse representation," IEEE Trans. On Cybernetics, vol. 46, no. 5, pp. 1132-1143, May. 2016.

[9]W. Hong, T. Chen, H. Wu, "An improved reversible data hiding in encrypted images using side match," IEEE Signal Processing Letters, vol. 19, no. 4, pp. 199- 202, Apr. 2012.

[10]Alka Dileep, K.Anusudha, Muhammed Asad P. T., " An Efficient Reversible Data Hiding Technique in Encrypted Images Based

on Chaotic Map," IEEE International Conference on Control Instrumentation, Communication and Computational Technologies,2015.

[11]. Wei Liu, WenjunZeng, Lina Dong, and Qiuming Yao "Efficient Compression of Encrypted Grayscale Images", Image Processing, IEEE Transactions Vol: 19, April 2010, pp. 1097 – 1102.

[12]. W. Puech, M. Chaumont and O. Strauss "A Reversible Data Hiding Method for EncryptedImages", SPIE, IS & T'08: SPIE Electronic Imaging, Security, Forensics, Steganography And Watermarking of Multimedia Contents, San Jose, CA, USA.

[13]. Christophe Guyeux, Nicolas Friot, and Jacques M. Bahi, "Chaotic iterations versus Spread-spectrum: chaos and stego security", January 25-2011, IIHMSP,pp. 208-211.

[14]. M. Johnson, P. Ishwar, V.M. Prabhakaran, D. Schonberg and K. Ramchandran, "On compressing and Systems for Video Technology, Vol. 13, No. 8, August 2003. pp. 890 - 896.

[15]. J. Tian, "Reversible data embedding using a difference expansion," IEEE Transaction on Circuits and Systems for Video Technology, Vol. 13, No. 8, August 2003. pp. 890 - 896.

[16]. PatrizioCampisi, Marco Carli, Gaeta no Giunta and Alessandro Neri, "Blind Quality Assessment System for Multimedia Communications using Tracing Watermarking" IEEE Transactions on Signal Processing, Vol 51, No 4, Apr 2003, pp. 996 – 1002.

[17]. S. Bounkong, B. Toch, D. Saad, and D. Lowe, "ICA for watermarking digital images," Journal of Machine Learning Research, vol. 1, pp. 1–25, 2002. [18]. G. Boatoa, F.G.B.DeNatalea, C. Fontana rib, F. Melgania"Hierarchical ownership and deterministic watermarking of digital images via polynomial interpolation", Signal Processing: Image Communication 21 (20 0 6), pp. 573–585.

[19]. A.H. Ouda, M.R. El-Jakka, "A practical version of Wong's watermarking technique", Proc. ICIP (2004) 2615–2618.

[20]. G. Boato, C. Fontanari, and F. Melgani "Hierarchical deterministic image watermarking via polynomial interpolation" Image Processing, 2005. ICIP 2005. IEEE International Conference on 11-14 Sept-2005,

[21]. H. Guo, N.D. Georganas, "A novel approach to digital image watermarking based on a generalized secret sharing scheme", Multimedia Systems 9 (3) (2003) 249.

[22]. Frederic Cerou, Pierre Del Moral, Teddy Furon and Arnaud Guyader, "Sequential Monte Carlo for rare event estimation" Statistics and Computing, pp. 1– 14, 2011.

[23]. F. Hartung, J. K. Su, and B. Girod, "Spread spectrum watermarking: Malicious attacks and counter attacks", Proc. SPIE, vol. 3657, pp. 147–158, Jan. 1999.

[24]. Mohanty S, Ramakrishna KR (1999) A dual watermarking technique for images." Proceedings of ACM Multimedia 1999, Orlando, 30 October–5 November 1999, pp 49–51.15.

[25]. M. Kankanahalli, et al., "Content Based Watermarkingfor Images", Proc. 6th ACM InternationalMultimedia Conference , ACM-MM 98, Sep. 1998, Bristol, UK, pp.61 - 70.