International Journal of Scientific Engineering and Technology Research

ISSN 2319-8885
Vol.05,Issue.21
August-2016,
Pages:4285-4292

www.ijsetr.com

Novel Method for Reversible Data Hiding using Steganography

DR. JOSEPH PRAKASH MOSIGANTI[1], ZAINAB SYED ZAMEERUDDIN[2]

[1]Professor, Dept of CSE, MCET, India, India, E-mail: dr.jpm7@gmail.com.

[1]PG Scholar, Dept of CSE, MCET, India, India, E-mail: zainab.syed06@gmail.com.

Abstract: The dire need of privacy, secrecy, security and protection has led to the substantial recognition of Steganography. Gary scale images were widely used for this purpose. Recovery of the encrypted image and hidden data without any loss has become the major requirement as, most of the previous methods could easily encrypt data and images but recovery was full of loss. By utilizing the redundancy within the image consummate performance can be attained. To obtain a massive hiding room, the pixels in the local structures such as a patch or a region can be excessively constricted because they have robust correspondence. This paper proposes to make use of a novel technique that is, sparse representation at the patch-level during the concealing of data so as to effectively investigate the association between adjacent pixels. In an over-complete dictionary, few atoms can linearly portray a patch by using sparse coding technique. The obtained residuary faults are encoded and self-embedded within the cover image because sparse coding is an estimation solution. Additionally, the encrypted image is also embedded with the learned dictionary. Due to the vigorous portrayal of sparse coding, an immense emptied room can be attained; consequently, the data hider can implant additional secret messages in the encrypted image. Commodious analysis manifest that the proposed method remarkably oversteps the state-of-the-art methods in terms of embedding rate and the image quality.

Keywords: Reversible Data Hiding (RDH), Image Encryption and Patch-Level Sparse Coding.

I. INTRODUCTION

Reversible data hiding (RDH) is one of the data hiding techniques whereby the host or original cover image and embedded secret message can be recovered absolutely and without loss of information. Being lossless makes this technique suitable for medical, legal scenarios and military applications where even a single disfigurement is not endurable. Image compression-based [1], [2], difference expansion based [3]–[7], histogram shift (HS)-based [8]–[11], image pixel pair based [12], [13], and dual/multi-image [14], [15] hiding methods are few RDH algorithms. Owing to the demand of privacy preservation [16], [17], prior to sending the content to the data administrator, the cover owner customarily encrypts the primitive content.Data administrator may want to embed supplementary messages into the encrypted image for authentication or steganography [18], despite not knowing the content of the original image. It's congenital and productive to use data hiding technique in encrypted image in this state. In military and medical frameworks it becomes obligatory not only to keep the content of the image concealed but also to recover it losslessly post the data extraction. Hence, RDH in encrypted images (RDHEIs) is worthwhile and preferable. Replacement of the three LSBs of the cover image with the message bits called as pixel-level compressive method is a common technique of manipulation of the least-significant-bit (LSB). In [23], the segmentation of the encrypted image is performed by dividing it into non-overlying blocks.

These blocks are divided into two sets. Flipping of three LSBs of a set is done for predefined pixels, which in turn gives rise to a single bit in a block. Hong et al. [24] gave an improved version based on [23]. While calculating the smoothness of every block, pixels are particularly harnessed and pixel association in the border of adjoining blocks is considered. This leads to reduction in the fault rate of the withdrawn bits. In [25], the constriction of the LSBs of the encrypted image is performed in order to create a sparse space to fit in some auxiliary data. It is difficult to squeeze space by only three LSBs. T hats why, T Zhang et al. [26] chose a half of fourth LSB as the space to carry the data. For the enhancement, Yin et al. [27] selected the smooth blocks in the encrypted image, and by using local HS, embedded the supplementary data into the blocks in an ordered manner with respect to block smoothness. The conserved spaces are all obtained by making use of LSB manipulation or constriction albeit the methods in [23]–[27] divide the image into patches or groups. This leads to the maximization of the entropy of the encrypted image and hence, it becomes tough to vacate the room losslessly after encryption, using the mentioned methods. Methods of reserving room before encryption (RRBE) are proposed [28], [29] to subjugate the above mentioned disadvantage. To do the estimation of the pixels, before encryption a huge chunk of pixels is used. The supplementary data is embedded in the encrypted image by working on the estimating errors.

In [29], the LSBs of some pixels are embedded into the other pixels and hence a reserving room is obtained. The three LSBs of the selected pixels is the extra space emptied out. This method has acquired superlative performance. The triumph of the above methods has substantiated that the data concealing can be achieved by utilizing the redundancy within the image. To make it more indistinguishable, only three LSBs can be used for data hiding though. As shown in Fig. 1(i), one patch with size A × A can hide 3A2 bits (3 bits per pixel). The image can be scrutinized at the patch level for many computer vision applications. Patches have merits pertaining to generalization and computation and they carry contextual data. Pixels in definite areas like patches consist of strong resemblance and the data in any image is associated inevitably. This gives us the power to perform constriction that results in a massive hiding room. Contemplating the two facets, to utilize the associations of adjacent pixels in a better way this paper proposes a novel method for high magnitude divisible reversible data concealing in encrypted images (HM_DRDCEI). As illustrated in the figure 1(ii) the substructure of room reserving before encryption is used. The image patch B is illustrated by sparse linear integrations of prototype signal atoms of an overcomplete dictionary D. Now only two things need space to record. They are: a few coefficients ˜w and the corresponding residuary fault ˜r Caused by sparse representation which gives rise to a higher capacity room.

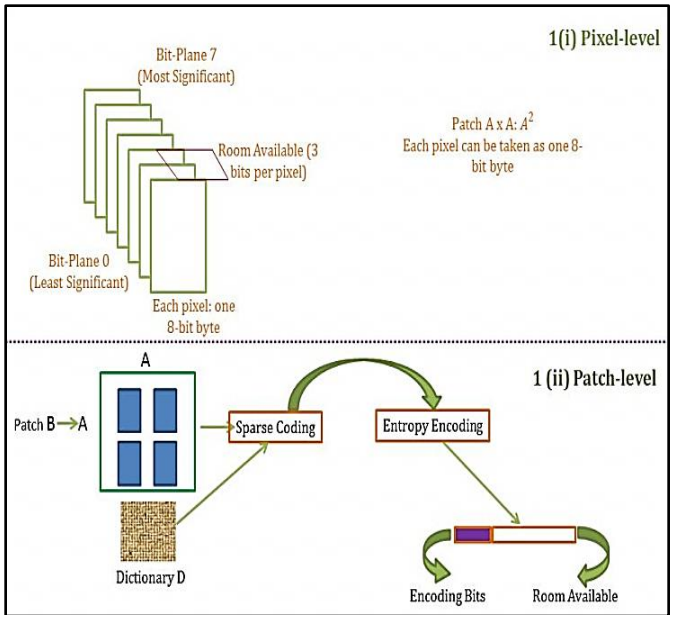

Fig.1. Contrast between pixel level and patch level.

Fig2 shows the flowchart of the proposed HM_DRDCEI method. The cover image is portrayed as per the over complete dictionary by the sparse coefficients to the data owner. Residuary faults and coefficients of the selected patches are encoded explicitly without quantization into the cover image. Doing this reduces the data size to a greater extent and therefore a massive empty room is made to conceal high magnitude data. The non-selected patches are embedded with residuary faults and learnt dictionary to recover the cover image flawlessly and further use respectively. When the recipient receives an encrypted image containing supplementary data, he/she can perform three functions. 1) He can extract the data without by using the data hiding key. 2) He can decrypt the image with a superior quality using the decryption key. 3) He can obtain both the data and cover image simultaneously provided he has both the keys.

II. RELATED WORK

One of the widely used techniques for Reversible Data Hiding in Encrypted Images is Reserving room before encryption. In [23], the cover image's encryption is first performed. After that, embedding of secret data is done by adjusting a tiny section of the encrypted image. At the end, the recipient first decrypts the encrypted image, and then extricates the embedded data and finally revives the original cover image. The disadvantage of this technique is that, each block is embedded only one bit payload. Furthermore, the block size is inversely proportional to the faulty bits of the data extraction. To subjugate this disadvantage, an improved RDHEI method using side match is proposed by Hong et al. [24]. To better approximate the smoothness of the blocks which is crucial for data extrication and image revival, this technique fully utilizes the pixels by adding up perpendicular and parallel differences in image blocks. Then, it arrogates the side match technique to join up the borders of the revived blocks to the other blocks. The fault rate obtained by this method is a bit lower. The feature Divisibility/ separability of RDHEI is not taken into consideration in either of these techniques. That is, data extrication and image revival should be happening separately. Zhang [25] proposed a novel scheme for separable RDHEIs. The data owner and data hider individually encrypt the original image by making use of encryption key and constrict the LSBs of encrypted image by making use of a data hiding key respectively to accommodate the supplementary data. In the recipient's side, three cases that the receiver has encryption and/or data hiding keys are considered.

By using LDPC code, lossless compression of the encrypted data can be performed as per Zhang's et al. [26] proposal. By making use of a coherent embedding procedure, the data hider constricts half of the fourth LSB in the cipher-text image, and lodges the compressed data and the supplementary data into the half of the fourth LSB. A faultless data extrication technique wherein multigranularity encryption is adopted after image partition is propounded by Yin et al. [27] the data hider chooses many smoother blocks for data embedding. Due to the increment in the entropy the room vacating becomes very tough. That's why all the above mentioned schemes obtain minute payloads. The MER in [23]–[27] are all less than 0.2 bits per second. Due to all these problems, instead of embedding data in encrypted images directly, Zhang et al. [28] proposed to estimate some pixels before encryption, and later on the supplementary data are embedded in the approximation errors. Furthermore, another technique, vacates room first by embedding LSBs of one pixel into the other. Due to which, these empty positions can b use to conceal data. This very useful scheme was put

forward by Ma et al. [29] this technique can differently extricate concealed data and decrypt the image. Furthermore, more than 10 times as large payloads as those of traditional techniques can be embedded. The extra space emptied out is limited to at most three LSB-planes per pixel though. Thus, the MER is only about 0.5 bits per second in [29]. The proposed HM_DRDCEI method inherits the merits of RRBE based on patch level sparse representation. The proposed method not only separates the data extrication from image decryption but also accomplishes excellent performance. Furthermore, unlike the previous techniques that majorly used pixel-level constriction feature, our scheme takes the patches as a whole, and represents them using sparse coding. Due to this, a high magnitude is achieved.

III. PROPOSED METHOD

In this section, a detailed introduction about HM_DRDCEI is given in three major aspects: 1) Generation of Encrypted Image; 2) Data concealing in the encrypted image; and 3) Data extrication and image revival. Color images with 8 bits per pixel are use.

A. Generation of Encrypted Image

Three phases are involved in the preparation of an encrypted image: a)Sparse representation; b) self-reversible embedding; and c) state (stream) encryption. Firstly, we take up the cover image and classify it into patches. Secondly, these patches are portrayed as per the over complete dictionary by making use of sparse coding. Thirdly, for room reservation, the smoother patches with lower residuary faults are selected. These chosen patches are illustrated by the sparse coefficients, and the corresponding residuary faults are encoded and reversibly embedded into the other not chosen patches with a standard RDH algorithm. Finally, the encryption is performed to get the final version.

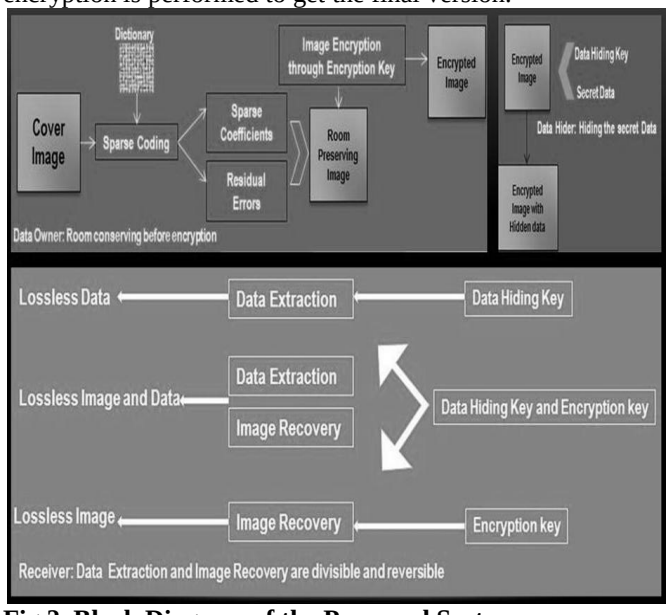

Fig.2. Block Diagram of the Proposed System.

Sparse Representation: Based on K-means singular value decomposition algorithm [33], the dictionary is trained so as to reserve a room to hide data. This leads to sparse signal representation as shown in Fig2. The training of the dictionary is an offline procedure and is fixed for the data hiding process. Given a cover image C with size A1 × A2, we first classify it into a bunch of non-overlapped A × A patches. The patch size A is set to 4 as default in our algorithm. Denote F as the number of patches of C, and F = A1 × A2/A × A. Vectorization of pixel values is done for each patch. The vectorization is performed as Bi∈ Rn×1 (i = 1, 2, . . . , F, and n = A2). Therefore, the image C ∈Rn×F, which contains F column vectors {Bi}Fi =1. Using an over complete dictionary matrix D ∈Rn×K(K > n) that contains K prototype signal atoms for columns, {dj}Kj=1, every image patch Bi can be represented as a sparse linear combination of these atoms as follows:

$$\min_{x_i} \|y_i - Dx_i\|_2^2 \quad subject\ to \quad \|x_i\|_0 \le L \qquad (1)$$

Where || • ||0 is the l 0 norm, counting the nonzero entries of a vector. L is a predetermined number of nonzero entries. The coefficient vector wi∈ RK×1 contains the representation coefficients of Bi, and is expected to be sparse. The well trained dictionary D can be used for any cover image.

Actually, the approximation of Bi using Dwi needs not to be exact, and could absorb a moderate error. In other words, the representation of Bi may be either exact Bi = Dxi or approximate, Bi ≈ Dwi. This suggests an approximation that trades off accuracy of representation with its simplicity. Therefore, we make an error correction step for lossless image recovery. Furthermore, the sparse coefficients wi are adjusted to integers $\tilde{w}i$ = round(wi) for the convenience of encoding. Therefore, Bi can be reconstructed by:

$$B_i = \text{round}(D\,\tilde{w}_i) + \tilde{r}_i \qquad (2)$$

where i = 1, 2, . . . , F, $\tilde{w}_i \in Z^{K\times 1}$, and $\tilde{r}_i \in Z^{n\times 1}$. Here, $\tilde{r}_I$ is considered as the residuary fault, which contains two parts:1) The reconstructed fault caused by sparse coding and 2) The rounding fault. At the recipient's side, once $\tilde{w}_i$ and $\tilde{r}_i$ are received, we can exactly recover the image content. After fault rectification, binary encoding of coefficient and residuary fault$\tilde{r}_i$ is performed. But, for $\tilde{w}_i$ binary encoding is not performed for the zero coefficients (as most of them are zeroes). Let the nonzero coefficients be denoted by T. This T is encoded. As a result, indices $p_i \in Z^{T\times 1}$and nonzero coefficients value $u_i \in Z^{T\times 1}$are used to characterize the coefficient $\tilde{w}_i$. The position p_i, is transformed into a number of position bits (n_i^p bits) which is equal to [$\log_2 K$]. The extent of the dictionary D is *K*. The value bits n_i^uwhich are the complementary bits are used to represent u_i. u_i consists of 11 bits because the range of coefficient is always [−1024, 1023].The analogous faults are shifted to $\tilde{r}_i$. Context-based adaptive variable length coding [35], [36] is used to encode the residuary fault $\tilde{r}_i n_i^r$ is used to signify the ultimate number of encoded bits for faulty bits, which may vary with the varying textures.

Self-Reversible Embedding: Room reservation is the next step. To do this various patches are chosen to create a regularized domain, G and G∈Rn×C. This domain consists of C column vectors represented by $\{\boldsymbol{y_k}\}_{k=1}^{c}$is considered to be the selected patch number, and the size of domain G is nC.

The criteria considered while selecting the regularized patches are i) Simple to represent patches ii) Patches containing tiny faulty bits. To add up, the binary value of flag bit Fiis considered while choosing the patches. This is computed as follows:

$$F_i = \frac{sign(n_i^g - \delta)+1}{2} \quad (3)$$

Selection of a patch is denoted by Fi=0 and the threshold for selection is denominated by which is computed as follows:

$$\delta = q[C], q = (4) \begin{pmatrix} n^e_{\varphi(1)} \\ n^e_{\varphi(2)} \\ \cdots \\ n^e_{\varphi(S)} \end{pmatrix} \quad (4)$$

In the above equation; C= selected patch number q= sorting result of nei in the ascending order, i, (i) = 1, 2, …..S.

One more parameter is required for the location of the next chosen regularized patches. This parameter involves another n_k^b bits. The encrypted mage is embedded with the position of initially chosen patch. The positions of the other chosen patches are calculated by using the following equation:

$$p_{x_k} = \begin{cases} \frac{p_k}{A_2/A_1} & mod(p_k, A_2/A_1) = 0 \\ floor\left(\frac{p_k}{A_2/A_1}\right) + 1, & mod(p_k, A_2/A_1) \neq 0 \end{cases} \quad (5)$$

$$p_{y_k} = \begin{cases} A_2/A_1 & mod(p_k, A_2/A_1) = 0 \\ mod(p_k, A_2/A_1) & mod(p_k, A_2/A_1) \neq 0 \end{cases} \quad (6)$$

na bits are required to embed the encrypted dictionary. The size of the concealed data is supposed to be M. The following shows the affinity between concealed data's size (M), patch number of the selected patch (C) and room preserving per patch (nd).

$$\frac{M}{n^d} = \left\lceil \frac{M}{8N^2 - L(n^p - n^v) - n^b - \tilde{n}^a} \right\rceil \quad (7)$$

$$C = \left\lceil \frac{M + n^a}{8A^2 - U} \right\rceil \quad (8)$$

where

$$U = L(\lceil log_2 K \rceil + 11) + \left(\left\lceil log_2 \frac{A1}{A} \right\rceil + \left\lceil log_2 \frac{A2}{A} \right\rceil \right) \quad (9)$$

By doing this, the cover image is transformed into a self-embedded and room preserved version Cc. Ultimately, sparse coefficients are used to portray the chosen patches. Arbitrary bits are used to fill up the space for parameter bits and dictionary bits. Post encryption, parameter bits and dictionary bits are settled and the emptied room is maintained for the data concealer. An area B is built with the help of standard RDH algorithm [37]. This area (B) is created because of the reversible embedding of the residuary faults into the rejected patches. This step is taken for lossless image revival. This area is quantified as follows: AB1×AB2, where

$$A_{B1} = A \times floor((S-C)/(A_2-A_1)) \quad (10)$$

AB2=A2

Image Encryption: State (Stream) cipher is used to originate an encrypted image Ce from the previously created image Cc. Eight bits of the pixel are denoted as follows: pi,j(i = 1, 2, . . . A1, j = 1, 2, . . . A2) as bi,j,0, bi,j,1, bi,j,2, bi,j,3, bi,j,4, bi,j,5, bi,j,6, and bi,j,7. Thus

$$b_{i,j,k} = \_p_{i,j}/2^m\_ \bmod 2,\ m = 0, 1, \ldots, 7 \quad (11)$$

Then, the encrypted bit stream can be expressed as follows:

$$b_{i,j,m} = b_{i,j,m} \oplus r_{i,j,m},\ m = 0, 1, \ldots, 7 \quad (12)$$

Where ri,j,m is a pseudo-arbitrary bit generated by the encryption key K_e. To notify the data concealer about the locations of the succeeding patches, the parameter bits are set into the chosen patches that can be embedded. The dictionary's encoding bits are also encrypted and embedded into the relative reserving room. Then, the embedding process of initially selected patch and the emptied room is also performed. By making use of either encryption key or data hiding key, the position can be decrypted. Conversely, data hiding size can be decrypted only by the data hiding key. Eventually, encrypted image Ce is acquired.

B. Data Concealing In The Encrypted Image

For authentication and administration purposes, the data hider can now embed any secret supplementary information in the received encrypted image. This process of embedding starts with finding the encrypted version of area A. The data hider effortlessly embeds data. After that, the data hider scans each selected patch in the encrypted image Ce, and simply makes use of bit replacement to substitute the corresponding bits reserved for secret data. Here, we assume the selected patch number is denoted as C, our MER for the data hider is computed as follows:

$$MER = \frac{C \times (8N^2 - L(n^p + n^v) - n^b) - n^a}{A_1 \times A_2} \quad (13)$$

C. Data Extraction and Image Recovery

With the encrypted image containing additional embedded data, the receiver faces three situations depending on whether the receiver has data hiding and/or encryption keys. The data extraction and image decryption can be processed separately.

Data Extraction with Only Data Hiding Key: For the receiver who only has data hiding key Kd, he first extracts and computes the starting position and the hiding room size for each patch and divides the received image into non-overlapped N × N patches. Then, data extraction is finished by checking the last nd bits for the selected patches in the received image. After that, all original hidden data are extracted and recovered with the data hiding key Kd. The extracted data is lossless.

Image Decryption with Only Encryption Key: In this case, the receiver has the encryption key Keonly. After extraction the position of the first selected patch by RDH algorithm, all the selected patches are identified one by one. Moreover, the dictionary D is also obtained by extraction. After patch

segmentation of the received image, the decryption procedure is performed and it includes two cases: 1) unselected patch decryption and 2) selected patch decryption. For unselected patch, the content can be directly decrypted according to the encryption

$$\text{key}bi,j,m = b \qquad i,j,m \oplus ri,j,m,\ m = 0 \ldots 7 \quad \textbf{(14)}$$

Where ri,j,m is the pseudo-random bit generated by the encryption key Ke. bi,j,m and bi,j,m are the encrypted bit and the decrypted bit for the pixel pi,j, respectively. Consequently, the unselected patch decryption is losslessly achieved. For the selected patch, we first decrypt the encoded bits by (14) based on encrypting Ke. Then, the position and value of the sparse coefficients for each selected patch {yk}_(k=1)^c are determined . After that , the corresponding coefficient, denoted as $\tilde{x}$k are obtained . Then, the decrypted patch y_k^d is computed via

$$y_k^d = \text{round}(D\tilde{x}_k) \quad \textbf{(15)}$$

Where k = 1, 2, . . . ,C, D is the trained dictionary. Since both the unselected and selected patches are decrypted, the image decryption in our proposed method is completed.

Data Extraction and Image Recovery with Both Data Hiding and Encryption Keys: If the receiver has both the data hiding key Kd and encryption key Ke, the data extraction[43-65] and image recovery achieve full reversibility. On the one hand, with the data hiding key Kd, one can extract the hidden secret data without any error. On the other hand, with the encryption key Ke, they first perform directly image decryption, then the corresponding coefficient for selected patches $yk\}_{k=1}^{c}$, denoted as $\tilde{x}$k , are obtained. After that, the residual errors $\tilde{e}$k , are extracted from the non selected patches (corresponding to area B). Therefore, the recovery patch yrk is computed as

$$y_k^r = \text{round}(D\tilde{x}_k) + \tilde{e}_k \quad \textbf{(16)}$$

Where k = 1, 2, . . . ,C. As the patch recovery is based on the lossless coefficients and residual errors, there exists no errors for the selected patches. Moreover, thanks to the RDH algorithm, the non selected patches are also recovered losslessly after residual errors extraction. That is to say, the image recovery in our proposed method is free of any error.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

Few experiments are carried out to analyse the propounded algorithm. The observations are as follows:

A. Dictionary Specifications

TABLE I:

VARIABLES	SPECIFICATIONS
Size of the image	4 x 4
No. of Patches	786 430
Image Type	RGB Color Image
Dictionary Trainer	K-Single Value Decomposition
Utmost Repetitions	48
Size of produced dictionary	16 x K
Coefficients' computation technique	Orthogonal Matching Pursuit (OMP)

Specifications: To enhance the selection of the dictionary specifications, the mean of faulty bits and position bits is computed. It is also observed that when T increments from 2 to 3 then, mean of bits increments from 103.62 to 108.77. Therefore the value of T is fixed to 2. The variable K controls the extent of position encoding and there is a directly proportional relationship between coefficients' encoding extent. K is adjusted and fixed to 64 because it is observe to exhibit best performance there. The training time in hours is as follows: at T=2 & T=3 (constant →) K=32 the time is 2.35 & 3.9 similarly, for K=64 time → 3.51 &3.06, for K=128 → 2.42 & 3.13, for K=256 time → 2.09 & 3.24 respectively.

B. Image Encoding

After obtaining a well-trained dictionary, the provided cover image can be portrayed in terms of sparse coding in accordance with obtained dictionary. Four images are chosen and with varying level of complexity in their textures. Encoding of the residuary faults is performed. The resulting images' pixels are in line with the extent of the encoding residuary faults. The pixels' brightness and the residuary faults caused by sparse representation are directly proportional to each other. The encoding method that is adopted gives us clear idea about the region of the image that can be easily portrayed by sparse coding. Apparently, simple textured patches are feasible for sparse coding when compared to complex ones. Our encoding strategy allows us to learn which part of the image or which type of image can be easily represented by sparse coding. Maximum frequency components may be present in the patches that will result in more number of residuary faults. Few patches are chosen and for data concealing and relative residuary errors are self - embedded. In our analysis, the patches with ER 0.1050, 0.2612 AND 0.573 are taken. Ultimately these selected patches are joined to give rise to an area for data concealing.

C. Reversible Data Concealing

Data concealers can conceal data upon receiving the encrypted image on specific demands. The image that we encrypted gave the result of ER = 0.93 bits per second. To extract the concealed data losslessly the data hiding key is required. Similarly, to obtain the decrypted image with good quality, encryption key is needed. With both the previously mentioned keys, both image and concealed data can be obtained without any loss, with higher quality. The recovered version and original version are similar visually to each other visually in addition to better image quality. In order to quantify the performance of the propounded system, it is compared with the other techniques available. This comparison proved that the technique we used id slightly better than the existing ones.

D. Evaluation of Computational Complexities

Choosing regularized area; self- reversible embedding; and image encryption are considered to be the most complex parts in terms of computations. We assume the gray-scale image with its size A1×A2, $\tilde{A}$= max(A1,A2).The computational complexity of regularized domain could be for [29] denoted by O (A2) + O($\tilde{A}$ log $\tilde{A}$).The first constituent

illustrates fault computing of the pixels, the second constituent illustrates regularized domain's sorting. The dictionary training and propounded data concealing algorithm should be explored or considered distinctly for image encryption while scrutinizing the computational complexities for the choosing of regularized domain. There are two phases in the training procedure. They are sparse coding and dictionary amendment. Both of these phases are prosecuted iteratively. As stated in [42], both phases can be done coherently in O(P/ATAKTS') = O(~A2TKTS'), where P is the number of pixels in the image (P = A1 × A2), A is the size of patch, T is the number of iterations, K is the number of atoms in the dictionary, T is the number of nonzero elements in each coefficient vector, and Sis the number of examples in the training set. K-SVD is fixed for the entire propounded process and it is an offline training process. Practically, non-optimized MATLAB code is used on a regular PC for the training process. Any user can preprocess this method by using any PC with common configuration. The computational complexity relies majorly on encoding that is sparse representation decoding that is patch recovery. OMP algorithm is used for encoding. A sort function is also required for ultimate regularized domain selection, which increases the computational complexity even more. The standard RDH algorithm is used for the other two steps: self-reversible embedding and image encryption and state encryption. Almost the same computational complexity is obtained.

V. CONCLUSION

A novel technique had been proposed in this paper, which takes up the advantages of divisibility property and of Reversible Data Hiding methods in the encrypted images. The room emptied for data concealing is very much utilized. A very simple technique of pixel relocation is used to fill up the given room with supplementary secret. The data extraction and image revival are all faultless and divisible. It has good potential and performance.

NOTE: This technique has been implemented using grey scale images so far. By referring other research papers there are no techniques that are implemented on RGB images. Here, in this paper I have implemented the same technique using a color image and the results and analysis are satisfactory.

Fututre Enhancements: Almost same techniques are used for the color images with a little variation in the code. Steganography in colored images is desirable and hence this enhancement could be done with the new techniques by just choosing a color image as the image cover and hiding the data. Appropriate coding and implementation would give excellent results if new methods/ algorithms are performed.

VI. REFERENCES

[1]M. U. Celik, G. Sharma, and A. M. Tekalp, "Lossless generalized- LSB data embedding," IEEE Trans. Image Process., vol. 14, no. 2, pp. 253–266, Feb. 2005.

[2]J. Fridrich, M. Goljan, and R. Du, "Invertible authentication watermark for JPEG images," in Proc. Inf. Technol. Coding Comput., Las Vegas, NV, USA, Apr. 2001, pp. 223–227.

[3]H. J. Kim, V. Sachnev, Y. Q. Shi, J. Nam, and H. G. Choo, "A novel difference expansion transform for reversible data embedding," IEEE Trans.Inf. Forensics Security, vol. 3, no. 3, pp. 456–465, Sep. 2008.

[4]D. Coltuc, "Improved embedding for prediction based reversible watermarking," IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 873 882, Sep. 2011.

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

[6] Y. Hu, H. K. Lee, K. Chen, and J. Li, "Difference expansion based reversible data hiding using two embedding directions," IEEE Trans.Multimedia, vol. 10, no. 8, pp. 1500–1511, Dec. 2008.

[7]B. Ou, X. Li, Y. Zhao, R. Ni, and Y.-Q. Shi, "Pairwise predictionerrorexpansion for efficient reversible data hiding," IEEE Trans. Image Process., vol. 22, no. 12, pp. 5010–5021, Dec. 2013.

[8]W. L. Tai, C. M. Yeh, and C. C. Chang, "Reversible data hiding basedon histogram modification of pixel differences," IEEE Trans. Circuits Syst. Video Technol., vol. 19, no. 6, pp. 906–910, Jun. 2009.

[9]C. C. Lin, W. L. Tai, and C. C. Chang, "Multilevel reversible data hiding based on histogram modification of difference images," PatternRecognit., vol. 41, no. 12, pp. 3582–3591, Dec. 2008.

[10]P. Tsai, Y. C. Hu, and H. L. Yeh, "Reversible image hiding scheme using predictive coding and histogram shifting," Signal Process., vol. 89, no. 6, pp. 1129–1143, Jun. 2009.

[11]S. L. Lin, C. F. Huang, M. H. Liou, and C. Y. Chen, "Improving histogram-based reversible information hiding by an optimal weightbased prediction scheme," J. Inf. Hiding Multimedia Signal Process., vol. 4, no. 1, pp. 19–33, Jan. 2013.

[12]S. W. Weng, Y. Zhao, R. R. Ni, and J. S. Pan, "Parity invariability based reversible watermarking," Electron. Lett., vol. 45, no. 20, pp. 1022–1023, Sep. 2009.

[13]S. Weng, Y. Zhao, J. S. Pan, and R. Ni, "Reversible watermarking based on invariability and adjustment on pixel pairs," IEEE Signal Process.Lett., vol. 15, no. 20, pp. 721–724, Dec. 2008.

[14]C. F. Lee and Y. L. Huang, "Reversible data hiding scheme based on dual stegano-images using orientation combinations," J. Telecommun.Syst., vol. 52, no. 4, pp. 2237–2247, 2013.

[15]G. Horng, Y. H. Huang, C. C. Chang, and Y. Liu, "(k, n)-image reversible data hiding," J. Inf. Hiding Multimedia Signal Process., vol. 5, no. 2, pp. 152–164, Apr. 2014.

[16]Y. Wang and K. N. Plataniotis, "An analysis of random projectionfor changeable and privacy-preserving biometric verification," IEEE Trans. Syst., Man, Cybern. B, Cybern., vol. 40, no. 5, pp. 1280–1293,Oct. 2010.

[17]Dabrowski, E. R. Weippl, and I. Echizen, "Framework based on privacy policy hiding for preventing unauthorized

face image processing,"in Proc. IEEE Int. Conf. Syst. Man Cybern. (SMC), Manchester, U.K., Oct. 2013, pp. 455–461.
[18]Y. T. Wu and F. Y. Shih, "Genetic algorithm based methodology forbreaking the steganalytic systems," IEEE Trans. Syst., Man, Cybern. B, Cybern., vol. 36, no. 1, pp. 24–31, Feb. 2006.
[19]X. Gao, C. Deng, X. Li, and D. Tao, "Geometric distortion insensitiveimage watermarking in affine covariant regions," IEEE Trans. Syst., Man,Cybern. C, Appl. Rev., vol. 40, no. 3, pp. 278–286, May 2010.
[20] M. S. Hsieh and D. C. Tseng, "Image subband coding using fuzzy inference and adaptive quantization," IEEE Trans. Syst., Man, Cybern. B,Cybern., vol. 33, no. 3, pp. 509–513, Jun. 2003.
[21]S. Lian, Z. Liu, Z. Ren, and H. Wang, "Commutative encryption andwatermarking in video compression," IEEE Trans. Circuits Syst. Video Technol., vol. 17, no. 6, pp. 774–778, Jun. 2007.
[22]M. Cancellaroet al., "A commutative digital image watermarking and encryption method in the tree structured Haar transform domain," SignalProcess. Image Commun., vol. 26, no. 1, pp. 1–12, Jan. 2011.
[23]X. Zhang, "Reversible data hiding in encrypted image," IEEE SignalProcess. Lett., vol. 18, no. 4, pp. 255–258, Apr. 2011.
[24]W. Hong, T. S. Chen, and H. Wu, "An improved reversible data hiding in encrypted images using side match," IEEE Signal Process. Lett., vol. 19,no. 4, pp. 199–202, Apr. 2012.
[25]X. Zhang, "Separable reversible data hiding in encrypted image," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 826–832, Apr. 2012.
[26]X. Zhang, Z. Qian, G. Feng, and Y. Ren, "Efficient reversible data hiding in encrypted images," J. Vis. Commun. Image Represent., vol. 25, no. 2, pp. 322–328, Feb. 2014.
[27]Z. Yin, B. Luo, and W. Hong, "Separable and error-free reversible data hiding in encrypted image with high payload," Sci. World J., vol. 2014, Mar. 2014, Art. ID 604876.
[28]W. Zhang, K. Ma, and N. Yu, "Reversibility improved data hiding in encrypted images," Signal Process., vol. 94, pp. 118–127, Jan. 2014.
[29]K. Ma, W. Zhang, X. Zhao, N. Yu, and F. Li, "Reversible data hiding in encrypted images by reserving room before encryption," IEEE Trans.Inf. Forensics Security, vol. 8, no. 3, pp. 553–562, Mar. 2013.
[30]W. Li, D. Zhang, Z. Liu, and X. Qiao, "Fast block-based image restoration employing the improved best neighborhood matching approach," IEEE Trans. Syst., Man, Cybern. A, Syst., Humans, vol. 35, no. 4, pp. 546–555, Jul. 2005.
[31]M. Johnson, P. Ishwar, V. Prabhakaran, D. Schonberg, and K. Ramchandran, "On compressing encrypted data," IEEE Trans. SignalProcess., vol. 52, no. 10, pp. 2992–3006, Oct. 2004.
[32]W. Liu, W. Zeng, L. Dong, and Q. Yao, "Efficient compression ofencrypted grayscale images," IEEE Trans. Image Process., vol. 19, no. 4, pp. 1097–1102, Apr. 2010.
[33]M. Aharon, M. Elad, and A. Bruckstein, "K-SVD: An algorithm for designing overcomplete dictionaries for sparse representation," IEEETrans. Signal Process., vol. 54, no. 11, pp. 4311–4322, Nov. 2006.
[34]R. Rubinstein, T. Peleg, and M. Elad, "Analysis K-SVD: A dictionary learning algorithm for the analysis sparse model," IEEE Trans. SignalProcess., vol. 61, no. 3, pp. 661–677, Feb. 2013.
[35]T. Wiegand, G. Sullivan, G. Bjontegaard, and A. Luthra, "Overview of the H.264/AVC video coding standard," IEEE Trans. Circuits Syst. VideoTechnol., vol. 13, no. 7, pp. 560–576, Jul. 2003.
[36]G. Sullivan and T. Wiegand, "Video compression—From concepts to the H.264/AVC standard," Proc. IEEE, vol. 93, no. 1, pp. 18–31, Jan. 2005.
[37]L. Luo, Z. Chen, M. Chen, X. Zeng, and Z. Xiong, "Reversible image watermarking using interpolation technique," IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, pp. 187–193, Mar. 2010.
[38]W. Stallings, Cryptography and Network Security: Principles and Practice, 3rd ed. Upper Saddle River, NJ, USA: Prentice-Hall, 2003.
[39]P. Bas, T. Filler, and T. Pevny, "'Break our steganographic system': The ins and outs of organizing BOSS," in Proc. 13th Int. Conf. Inf. HidingConf., Prague, Czech Republic, May 2011, pp. 59–70.
[40]M. Everingham, L. Van Gool, C. K. I. Williams, J. Winn, and A. Zisserman, "The PASCAL visual object classes (VOC) challenge," Int. J. Comput. Vis., vol. 88, no. 2, pp. 303–338, Jun. 2010.
[41]H. Jegou, M. Douze, and C. Schmid, "Hamming embedding and weak geometric consistency for large scale image search," in Proc.10th Eur. Conf. Comput. Vis. I (ECCV), Marseille, France, Oct. 2008, pp. 304–317.
[42]O. Bryt and M. Elad, "Compression of facial images using the K-SVD algorithm," J. Vis. Commun. Image Represent., vol. 19, no. 4, pp. 270–282, May 2008.
[43]Joseph Prakash"Innovative Pattern Based Morphological Method for Texture Segmentation-IEEE conference, Chennai, June 4-6, 2013, pp.11-15.
[44]Joseph Prakash"Texture Segmentation by a New Variant of Local Binary Pattern", in Advances in Intelligent Systems and Computing, Springer, Vol. 2, pp.385-392, ISSN 2194-5357, Springer, July 2015.
[45]Joseph Prakash"A Novel Approach for the Extraction of Tubercle Bacilli using Stationary Wavelet based Morphological Texture Segmentation", Intern. Conf. ICEPT 2016, Vol.1,pp.52-58, ISBN 978-93-5258-110-8, March 2016.
[46]Joseph Prakash"Morphological multiscale stationary wavelet transform based texture segmentation", International Journal Image, Graphics and Signal Processing, Vol. 6, No. 8, July 2014.
[47]Joseph Prakash"An Enhancement System for Efficient Driving", International Journal of Advanced Technology and Innovative Research Volume. 06, IssueNo.10, November-2014, Pages: 1242-1245 with impact factor of 2.12.
[48]Joseph Prakash"A New Texture Based Segmentation Method to Extract Object from Background", Global Journal of Computer Science and Technology Graphics & Vision, Volume 12, Issue 15 , Dec 2012, pp. 47-53.

[49]Joseph Prakash"Security for Multiparty Access in Online Social Networks", International Journal of Advanced Technology&Innovative Research Volume. 06, IssueNo.11, November-2014, Pages: 1280-1284, impact factor of 2.12.
[50]Joseph Prakash"Morphology Based Technique For Texture Enhancement and Segmentation", Signal & Image Processing: An International Journal, Volume 4, Number 1, Feb 2013, pp.49-56.
[51]Joseph Prakash"A Novel Approach for the Extraction of Tubercle Bacilli using Stationary Wavelet based Morphological Texture Segmentation" in International Conference on Rough Sets and Knowledge Technologies (accepted).
[52]Joseph Prakash"An Approach for Texture Segmentation based on Random Field Model and Wavelet Fusion", International Journal of Signal and Image Processing (IJSIP), Volume 1, Issue 3, May 2010, pp.183-189.(Free)
[53]Joseph Prakash"A New Approach for Texture Segmentation Using Gray Level Textons", International Journal of Signal and Image Processing (Free Journal), vol. 6, no. 3, June 2013, pp.81-89.
[54]Joseph Prakash"A Novel Approach for Texture Segmentation based on Mathematical morphology", Proceedings of International Conference on Recent Advances in Technology, Engineering, Management & Science (ICRATEMS-2011), Chennai, March 04-06, 2011, pp.270-275.
[55]JosephPrakash"AnInnovative Multicloud Implimentation of Computing Clusters for Loosely Coupled MTC Applications", International Journal of Technology and Engineering Science, Vol.1, No.8,pp: 1283-1290, Nov. 2013.
[56]Joseph Prakash"Segmentation of Medical texture images, International Conference on Recent Advances in Computer Science (ICRACS-2K12), GIET, 2012.
[57]Joseph Prakash"A Syntactic approach to ECG Analysis", International Conference on Emerging trends in Signal Processing & VLSI design at Gurunanak Engineering College, Hyderabad, June 11th to 13th 2010.
[58]Joseph Prakash"Fuzzy Random Impulse Noise Removal from Color Image Sequences", International Journal of Technology and Engineering Science [IJTES], Volume 1, Issue 8, pp: 1273-1276, November 2013.
[59]Joseph Prakash"Texture Segmentation based on Morphological Transforms", Proc. of National Seminar, Artificial Intelligence Applications of Image Processing, AIAIP-2K12,GEC, Vol. 1, No.1, August 2012, pp. 164-167.
[60]Joseph Prakash"Innovative Simplified Texture Spectrum for Texture Segmentation", ICRACS 2K12, Vol.No.1, 2012/March, Page Nos. 759-763.
[61]Joseph Prakash"Morphological image processing based Automatic Traffic control system" won 1st prize at NMREC, Hyderabad.
[62]Joseph Prakash"Data mining for web based educational system" won 1st prize at Conference Organized at Hyderabad.
[63]Joseph Prakash"Finger Ring Plethysmographic Sensors" Conference Organized by Bharath Deemed University, Chennai.
[64]Joseph Prakash"A New Method of Automatic and Accurate Image Registration through Histogram Based Image Segmentation", International Journal of Advanced and Innovative Research, Vol.2, No.9, Sept. 2013, pp. 439-446.
[65]Joseph Prakash"Wavelet approach for detecting clouds and their Shadows", International Journal of Latest Trends in Engineering and Technology, Vol. 3 Issue 1 September 2013, pp. 259-266.

Author's Profile:

Dr. Joseph Prakash Mosiganti received the B.E Degree from Andhra University and received his M. Tech. in Computer Science Engineering from JNTU College of Engineering, JNT University, Kukatpally, Hyderabad, India. He obtained Ph.D from JNTUK, He is having nearly 20 years of teaching, research and industrial experience. He taught courses for B.Tech and M.Tech students. He handled various positions Professor, HOD, I/C Principal, Co-coordinator, Currently with Methodist College of Engineering & Technology, Abids, Hyderabad, Affiliated to Osmania University, Hyderabad, India. He is NBA, NAAC Consultant. He has published 30+ research papers in various International Journals and conferences including IEEE, Springer. He won first prize for some of the presentation in conferences. He is a life member of CSI, ISTE, Red Cross and Indian Science Congress. He is Editorial Board member for SIPIJ, IJAET. He has been awarded with academic Excellency award, Educationist award, Research Excellence award, Seva Ratna award, Outstanding Councellor. His life's aim is to impart Character Education along with Excellence in academics with emphasis on Human Values and Ethics in educational institutes. He is service oriented counselor and prepares them to face the real life. He is dedicated and practical oriented teacher, his quality is creativity, self motivation, Godliness. He continuously learns and upgrades his skills; he says "if we are not updating ourselves we will be outdated". He shares his knowledge with students and staff. He is also involved in National Service activities, personality development, improving employability skills, distributing books and other needs for economically poor people in the society.

Zainab Syed Zameeruddin, Research Scholar, Department of CSE, pursuing of Masters in Technology from Methodist College Engineering and Technology, affiliated to OsmaniaUniversity, Hyderabad, She obtained her Bachelor's degree in Computer Science from Deccan College of Engineering and Technology, affiliated to Osmania University, Hyderabad, India. Her research interests include information security, Data Hiding, Steganography, and Cloud Computing. She had executed one major project wherein she successfully implemented an IEEE technical paper "Enhanced Data Security Model for Cloud Computing". She actively participates in research work and also works as an IT Facilitator for the CSR project at SMART centre, Tech Mahindra Foundation. She trains under-privileged youth in IT skills. She has a firm belief "Hard work and success go hand in hand".