Reversible Data Hiding in Encrypted Images using Interpolation-based Distributed Space Reservation

Shwetha S N[1], Chaithrashree C G[2], Lakshmishree B S[3], Lakshmidevi A B[4],Rakshitha R K[5], 'assistant

Professor, [2345] UG Students Department of Computer Science and Engineering BGS Institute of

Technology, B G Nagar

Abstract-Reversible data hiding (RDH) in scrambled pictures has achieved more consideration as of late in explore group. Security assurance of extra information and additionally cover media makes it appealing for applications in therapeutic imaging, distributed storage, crime scene investigation and so on. In this paper, another strategy for reversible information stowing away in encoded pictures (RDH-EI), is proposed. Our strategy receives the approach of holding adequate space for the extra information before encoding the cover picture. To start with we distinguish appropriate pieces for concealing information from different parts of the picture. Before scrambling the picture, at least one LSB-planes of these squares are went down into outstanding parts of the picture utilizing a high-performing conventional RDH strategy that takes a shot at decoded pictures. In the wake of encoding the picture, those LSB-planes are utilized to shroud extra information. Recuperation of unique cover picture and blunder free extraction of extra information is ensured dependably. In addition, the proposed technique is straightforward and natural. Tentatively outcomes demonstrate that our technique out-plays out the best in class strategies for reversible information covering up in encoded pictures.

Keywords-Reversible data hiding; interpolation; encryption; histogram; reservation

I. INTRODUCTION

Reversible data hiding (RDH) involves hiding data into a cover medium in a manner that the original cover medium can be recovered from the distorted stego medium [1]. This has been a focus area of research for decades. Method [2] patented by Barton is one of the earliest techniques in RDH. It was used for authentication of digital content using digital signature embedded into the content. Theoretical analysis on capacity limits of RDH is done by Kalker *et al.* [4]. RDH is performed using different kinds of cover media such as images, videos, audio etc. Among them, digital image have been a popular choice as cover medium. RDH using digital images finds application in military imaging, medical imaging, forensics etc. since permanent distortion to cover image is unacceptable in these areas.

If the data hidden is some information related to cover medium itself, it is called watermarking. This is usually done for authentication and copyright protection. A classification of reversible watermarking schemes is done by Feng *et al.* [5]. This is generally applicable to RDH also. First category uses technique known as difference expansion as in case of [6]-[8]. These methods generally work by expanding small values, such as neighboring pixel difference, to embed additional bits. Second category of techniques uses compression of cover medium to find room for additional data[11]. Histogram shifting is used in the third category of techniques [12], [13].Some of the recent techniques [14], [15] use a combination of the above three approaches.

Traditional RDH techniques do not protect the privacy of the cover image. Sometimes it is necessary to ensure privacy of cover image and at the same time hide additional data into it. Medical imaging, cloud storage, forensics etc. are some of the application areas where such requirements are common. Reversible data hiding in encrypted images (RDH-EI) is used for this purpose. In RDH-EI, the cover image is encrypted first and then additional data is hidden into it. A desirable property of RDH-EI is the severability of encryption and data hiding. It means that these two operations can be done by two different individuals. This way the data hider can be kept out of viewing the cover image content. Similarly, separability in data-extraction and image recovery is also highly sought. This property can enhance the scope of RDH-EI.

There are two main approaches for RDH-EI as classified in

First approach is to encrypt cover image and then find ways to hide additional data in the encrypted image. Methods [16]-[18] fall in this category. Limitations of these methods are low data hiding capacity and conditional reversibility. Since the entropy is maximized for encrypted images, it is difficult to find more space for additional using compression, pixel correlation etc. Also, error-free extraction of data and reversibility of cover image may not be possible at high embedding rates. Method [19] improved embedding capacity and ensured true reversibility for all cases. Even then the achieved capacity is not significantly high for this approach, which limits the practical applications for these methods. The second approach is to reserve space for additional data in a lossless manner before encrypting the image. This space can be used to hide additional data after encrypting the image. Ma *et al.* [21] proposed a method that follows this approach which gives significant improvement in embedding capacity and also real reversibility in all cases.

Also, separability is ensured in both embedding and extraction process. In this paper we propose a method that adopts the second approach. Has got several demerits. In fact [20] performs better for a smooth image. But since a single large region is chosen as , a lot of smooth areas become part of and coarse areas in as clearly seen in Fig. 1(b).This effects in in a reduced performance of [20] on [21]. Moreover, restructuring of the cover image is must be performed in embedding and extraction sides to get a meaningful stego image and also to recover cover image. This is rather unintuitive. Another problem is that the method of selecting the region is computationally intensive as it works in a sliding-window manner and compute smoothness factor on each window of pixels.

Strategy [21] was enhanced by the creator utilizing a procedure alluded as dynamic square trade [22]. In this strategy, a novel way is utilized to quantify the coarseness of non-covering hinders in the picture. Exceptionally coarse squares are the moved to start of the picture coming about all coarse piece gather in the best area of the picture as appeared in Fig. 1(c). The rest of the picture ends up being more reasonable for strategy [20] to shroud more information with less disintegration in PSNR. Technique [22] is perplexing in itself because of unintuitive improvement of picture squares which includes additional means in sender and beneficiary side

II. PROPOSED METHOD

The proposed strategy chooses appropriate pieces from various parts of the picture to conceal extra information. Dissimilar to different techniques [21] and [22], the chose pieces are not moved; consequently the first structure of the cover picture is unaffected. At least one LSB - planes of these bocks are extricated and reversibly inserted into residual districts of the picture utilizing a customary RDH strategy [20] which works for decoded pictures. The picture is then encoded and those went down LSB-planes are utilized to shroud extra information. We utilize a novel method to choose adequate number of little measured coarse pieces to conceal extra information, which in actuality makes remaining picture area more reasonable for [20] than with the parceling approach in [21]. Our strategy is made less complex and more instinctive by abstaining from rebuilding of the picture. The held squares stay in their unique positions in the cover picture. To adapt to highlight, technique [20] is changed and utilized as a part of the proposed strategy.

This area depicts the proposed technique in detail. Let mean the arrangement of squares saved and the staying open locales of the picture together is meant as . Initially we portray the introduction procedure utilized as a part of our technique. This is a rearranged adjustment of the interjection utilized as a part of [21] to suit our strategy. After that determination procedure for the squares is clarified. This is trailed by the space reservation step

A. Pixel Interpolation

The interpolation technique used in the proposed method is a simplified adaptation of the interpolation used in [21], to suit our method. There two cases for the interpolation of current pixel based on whether is an interior pixel or a border pixel. Interpolation of interior pixel: Interpolated value ’ for is computed as a weighted average of the horizontal and vertical The insertion procedure utilized as a part of the proposed technique is a streamlined adjustment of the addition utilized as a part of [21], to suit our strategy. There two cases for the insertion of current pixel in light of whether is an inside pixel or a fringe pixel.

Given a region of an image, we can compute interpolation- error for every pixel in the in the block and plot interpolation-error histogram as shown in Fig. 3. In [20], pixels in the two peak points and of this histogram are used for embed bits by a process of additive interpolation- error expansion. Higher the number of pixels in these bins (i.e., a sharper histogram for the region), we can embed more bits in that region. So we choose the reserved block set such that it comprises of the blocks that contribute least number of pixels to the peak bins and which in turn results in a better for [20].

B. Selection of blocks for data hiding

In this step, first the cover image is divided into blocks of size where denotes the length additional data to hide. Set generally a singleton since the metadata is normally is of small length and Let be the total number of blocks in the image, then number of bits required to rep where denotes the length additional data to hide. Set generally a singleton since the metadata is normally is of small length and hence = 1 . Let be the total number of blocks in the image, then number of bits required to represent a block index is given by resent a block index size is given by

Fig. 1. (a) Original Lena image. (b) Partitioning in [21]. (c) Output of active block exchange (ABE) in [22]. (d)

DSR in proposed method.

where denotes the length additional data to hide. Set generally a singleton since the metadata is normally is of small length and hence = 1 . Let be the total number of blocks in the image, then number of bits required to represent a block index is given by

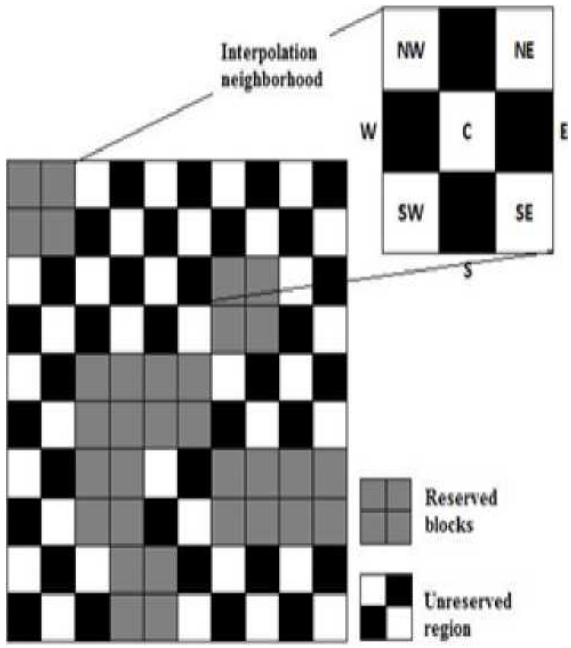

Fig. 2. Blueprint of reserved blocks and unreserved blocks distribution in an image with interpolation neighborhood highlighted.

rest of the blocks, + blocks with least values for are chosen as the data bock set and metadata block set . Fig. x4 shows the outline of the blocks reserved in Lena for a embedding rate of 0.3 bpp (bits per pixel) and = 1. In effect we choose those blocks which contribute the least number of pixels to the peak bins, to reserve space for additional data.

This increase the prospect of sharper interpolation-error histogram for the remaining unreserved region and hence better performance for [20] when applied to With these modifications, we use additive interpolation-error expansion in [20] to reversibly embed original LSB-planes of reserved blocks into and to use those LSB-planes to hide additional data. Additive interpolation-error expansion function.

C. Space reservation for additional data

Once the reserved blocks are chosen using previous step, LSB planes of the blocks in set are extracted and reversibly embedded in region using modified version of traditional RDH method [20]. Modifications applied to [20] are in the following aspect.

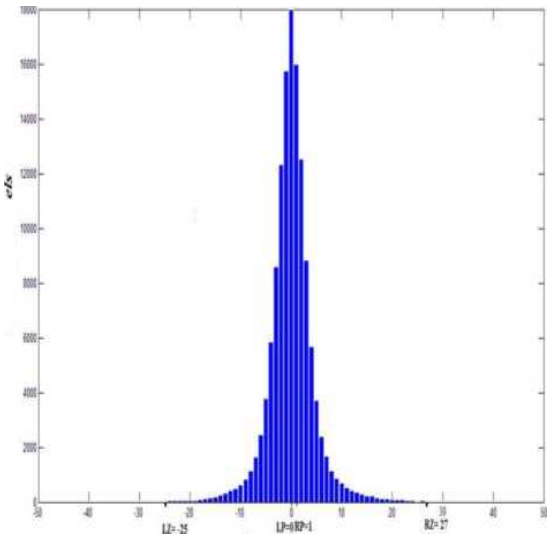

Fig 3. Interpolation-error histogram for Lena image with peak points LP = 0 and RP=1.

1 .Pixel interjection: Dissimilar to unique [20], the outskirt pixels of are likewise inserted and thus used to store extra information. The pixels which are neighbouring held squares are additionally regarded as outskirt pixels.

2 .Metadata capacity: In [20], metadata required in extraction process are put away into LSB-planes of fringe pixels, while, the proposed strategy stores it in LSB-planes held pieces in set .

3. Two-pass implanting: To misuse all pixels in for bit installing, one round of finish inserting into is part into two stages. In this first stage every one of the pixels.

4 .Method [20] for the most part chips away at rectangular picture area, while, in our technique locale require not be rectangular, since held pieces ( ) are conveyed over the cover picture.

D. Encryption of cover image

In the wake of saving space for extra information, the cover picture encoded. Encryption plot is same as the one utilized as a part of where a stream figure is utilized. Pseudo-irregular number grouping (x) is produced utilizing an encryption key ( ). Bitwise restrictive OR activity of pixel esteems and comparing pseudo- arbitrary number of the created grouping is utilized for encryption. it is clear that only those pixels belong to two peak bins LP and RP of the interpolation-error histogram are used for bit embedding. Function. The stego pixel is obtained from interpolated pixels value.

Multiple rounds of bit embedding can be done in *UR*, taking output image of one round as the cover image for next round, depending on the length of additional data to hide. Overflow and underflow scenarios are handled.

E. Hiding additional data in reserved space.

LSB-planes of the reserved blocks in set *DB* are now

available to store additional data. The data is encrypted using a data-hiding key ( ) before storing. If data-hider is different from content owner, he is provided with the indices of the reserved blocks, and number of LSB-planes (n) available. In addition to that, content owner or data-hider need to store the indices of reserved blocks (members of *DB* and *MB*) into LSB-planes of the reserved index blocks (set *IB*) which are the starting blocks of the cover image. This information is required in the extraction process to identify the all the reserved blocks. Index data may be encrypted using a separate key to ensure additional protection. The image obtained as a result of this step.

F. Extraction process

Extraction process involves recovering the additional data and restoring the original cover image. The steps are more-or-less the reverse of embedding process as summarized below using a boundary map, same way as [20]. Boundary map, values of *LP*, *RP*, *LZ*, *RZ* and number of embedding rounds, form the metadata and are embedded into *n* LSB-planes of blocks in set *MB*. These are required for the image recovery at extraction side. The image obtained as a result of this step.

For every pixel interpolation-error computed using (3). *b* is the bit to embed. *LZ* and *RZ* are the first zero-bins towards left and right of *LP* and *RP*. LSB-planes of blocks in *RB* and *IB* excepted while decrypting to preserve the additional data and block indices. Decrypted image is used to measure the distortion introduced on the original image by the embedding process.

Recovering original cover image: This step mainly involves extracting the bits embedded in the region *UR* of using extraction procedure of [20] applied in the reverse order i.e., first pixels marked as black(Fig x5) are processed followed by white pixels. A brief explanation is given here. For a stego pixel ” £ the interpolated value using the same interpolation steps as in embedding process. Expanded interpolation-error.

In this way, all the pixels region UR of original cover image is recovered and the bits embedded are extracted. The extracted bits are then placed into the LSB-planes of blocks in set *RB* to obtain the original cover image.

III. EXPERIMENAL RESULTS

The proposed method is tested using the publicly available standard test images Airplane, Baboon, Lena, and Wine from database [23]. These test images represent the classes of natural images varying from smooth images (e.g. Airplane) to highly textured images (e.g. Baboon). Table I is a comparison of the performance of the proposed method with methods [21] and [22]. Test results, for embedding rates from 0.1 bpp to 0.6 bpp, are shown in terms of PSNR values of the directly decrypted stego images. In most of the cases the PSNR value given by the proposed method is larger than that of methods and [22] by up to 3 db. At lower embedding rates such as 0.1 bpp, 0.2 bpp etc., the improvement in the PSNR is smaller. This is s because, at small embedding rates, the number of blocks required for hiding the additional data is small and that results in lesser impact for the block selection approach we employ.

At higher embedding rates the required blocks are more and the effectiveness of our mechanism to select the suitable blocks is more explicit in such cases. Among the test images used, the image Wine and Baboon deserves special mention. Wine image gives highest PSNR values for a given embedding rates. This is because the image has plenty of smooth regions where traditional RDH method [20] performs exceptionally well. Smooth regions result in more accurate interpolation and hence contribute to the peak bins of the interpolation-error histogram.

In contrast, highly textured image Baboon gives lowest PSNR values for given embedding rate. The reason is obviously the poor performance of method [20] for textured image. Graph in Fig. 4 shows the comparison of embedding capacities when the PSNR values of the stego images are maintained in a reasonable quality range of 35 dB to 40 dB. . From the graph it is clear that the proposed method gives improved embedding capacity of over 10000 bits. While the improvement in capacity is less for Baboon, the most textured image among the samples, images like Airplane, Lena, Wine etc. having mix of smooth and textured regions, give high improvements in capacity.

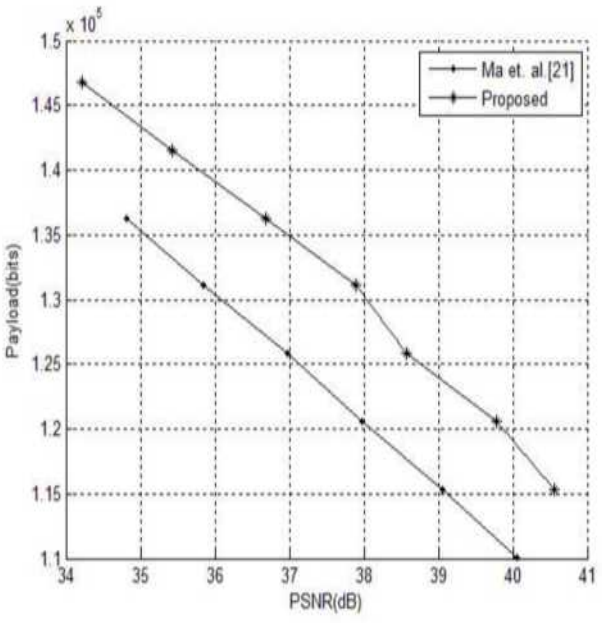

Figure 4. Comparison of embedding capacity (bits) when PSNR of decrypted stego image is maintained the range 35-41 dB for Lena

TABLE I COMPARISON OF PSNR VALUES AT VARIOUS EMBEDDING RATES (BITS-PER-PIXEL, BPP) FOR METHOD [21] ,[22] AND PROPOSED METHOD.

			Embedding					
Test Image	**Layers**	**Method**	0.1	0.2	0.3	0.4	0.5	0.6
Airplane	1	Method [21]	54.21	50.98	48.26	44.67	40.78	34.52
		Method [22]	54.13	51.21	49.36	45.92	42.06	36.31
		Proposed	**54.21**	**51.44**	**49.89**	**46.15**	**42.55**	**37.37**
	2	Method [21]	53.04	49.86	48.11	45.05	42.73	40.48
		Method [22]	53.04	49.94	48.22	45.57	43.57	40.91
		Proposed	**53.06**	**50.11**	**48.36**	**45.82**	**43.74**	**41.74**
Baboon	1	Method[21]	46.17	40.68	35.86	31.33	26.26	19.20
		Method [22]	46.27	40.85	36.81	32.69	28.52	22.65
		Proposed	46.24	**40.93**	36.49	32.61	**28.62**	**22.83**
	2	Method[21]	45.92	40.41	36.47	33.08	29.82	27.06
		Method [22]	45.92	40.5	36.71	33.28	30.27	27.66
		Proposed	45.88	**40.62**	**36.71**	**33.41**	**30.27**	27.65
Lena	1	Method[21]	52.32	49.07	45.00	40.65	35.84	30.02
		Method [22]	52.42	49.39	45.84	41.81	37.64	31.19
		Proposed	**52.59**	**49.62**	**45.84**	**42.59**	**37.89**	**32.01**
	2	Method[21]	51.53	48.39	45.09	42.56	39.46	36.44
		Method [22]	51.57	48.49	45.4	42.98	40.45	37.63
		Proposed	**51.70**	**48.63**	**45.46**	**43.32**	**40.95**	**38.12**
Wine	1	Method[21]	54.83	52.07	50.32	47.17	43.29	37.58
		Method [22]	54.99	52.50	51.16	48.85	45.83	40.85
		Proposed	**55.43**	**52.97**	**51.45**	**50.27**	**46.55**	**41.76**
	2	Method[21]	53.58	50.69	48.90	47.74	45.01	42.92
		Method [22]	53.55	50.87	49.14	48.05	46.41	44.51
		Proposed	**53.78**	**51.12**	**49.48**	**48.35**	**46.95**	**45.07**

Figure 4. Comparison of embedding capacity (bits) when PSNR of decrypted stego image is maintained the range 35-41 dB for Lena

IV. CONCLUSION

The proposed technique is for reversible information stowing away in scrambled images (RDH-EI). By receiving the approach of saving space for extra information before encryption, this strategy accomplishes preferred execution over the current techniques as far as PSNR of the stego picture and inserting limit. These qualities make this strategy appropriate for pragmatic applications in medicinal imaging, military imaging and so forth. Also, this strategy is straightforward and simple to execute contrasted with its antecedents. This is on the grounds that we are dispensing with the requirement for rebuilding the picture dissimilar to alternate techniques in writing. For the majority of the pictures the installing limit with regards to extra information is enhanced past 10000 bits. In the meantime, on the off chance that we think about the PSNR of stego picture by keeping the information installed consistent, there are eminent changes in PSNR for every one of the pictures over the detail of-the craftsmanship techniques.

REFERENCES

[1] C. W. Honsinger, P. W. Jones, M. Rabbani, and J. C. Stoffel, “Lossless recovery of an original image

containing embedded data," U.S. Patent 6 278 791, 2001.

[2] J. M. Barton, "Method and Apparatus for Embedding Authentication Information Within Digital Data," U.S. Patent 5 646 997, 1997.

[3] Z. Ni, Y. Q. Shi, N. Ansari, and S. Wei, "Reversible data hiding," in ISCAS Proceedings of the 2003 International Symposium on Circuits and Systems, vol. 2, pp. II—912—II— 915, Thailand, May 2003.

[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] J. B. Feng, I. C. Lin, C. S. Tsai, and Y. P. Chu, "Reversible watermarking: Current status and key issues," Int. J. Netw. Security, vol. 12, no. 3, pp. 161-171, 2006.

[6] A. M. Alattar, "Reversible watermark using the difference expansion of a generalized integer transform," IEEE Transactions on Image Processing, vol. 13, no. 8, pp. 11471156, Aug. 2004.

[7] J. Tian, "Reversible data embedding using a difference expansion," IEEE Transactions on Circuits Systems and Video Technology, vol. 13, no. 8, pp. 890-896, Aug. 2003.

[8] D. M. Thodi and J. J. Rodriguez, "Reversible watermarking by prediction-error expansion," in Proceedings of the 6th IEEE Southwest Symposium on Image Analysis and Interpretation, vol. 3.

[9] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Lossless generalized-lsb data embedding," IEEE Transactions on Image Processing, vol. 14, no. 2, pp. 253-266, Feb. 2005.

[10] J. Fridrich and M. Goljan, "Lossless data embedding for all image formats," in SPIE Proceedings of Photonics West, Electronic Imaging, Security and Watermarking of Multimedia Contents, vol. 4675, pp. 572-583, San Jose, Jan. 2002.194

[11] G. Xuan, C. Yang, Y. Zhen, Y. Q. Shi, and Z. Ni, "Reversible data hiding based on wavelet spread spectrum," in Proceedings of the IEEE 6th Workshop on Multimedia Signal Processing, pp. 211-214, Italy, Sept. 2004.

[12] C. D. Vleeschouwer, J. E. Delaigle, and B. Macq, "Circular interpretation of histogram for reversible watermarking," in Proceedings of the IEEE 4th Workshop on Multimedia Signal Processing, pp. 345-350, France, Oct. 2001.

[13] B. Yang, M. Schmucker, X. Niu, C. Busch, and S. Sun, "Reversible image watermarking by histogram modification for integer dct coefficients," in Proceedings of the IEEE 6th Workshop on Multimedia Signal Processing, pp. 143-146, Siena, Italy, Sept. 2004.

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

[15] V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y. Q. Shi, "Reversible watermarking algorithm using sorting and prediction," IEEE Trans. Circuits Syst. Video Technol., vol. 19, no. 7, pp. 989-999, Jul. 2009.

[16] X. Zhang, "Reversible data hiding in encrypted images," IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255-258, Apr. 2011.

[17] W. Hong, T. 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.

[18] X. Zhang, "Separable reversible data hiding in encrypted image," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 826-832, Apr. 2012.

[19] N. S. Nair, T. Mathew, Neethu A.S., Viswajith P. Viswanath, Madhu S. Nair, M. Wilscy, "A Proactive Approach to Reversible Data Hiding in Encrypted Images", Procedia Computer Science, Elsevier, Vol.46, pp. 1510-1517, 2015