DOI: 10.21917/ijivp.2011.0036

COLOUR IMAGE STEGANOGRAPHY USING MEDIAN MAINTENANCE

S. Arivazhagan[1], W. Sylvia Lilly Jebarani[2] and S. Bagavath[3]
Department of Electronics and Communication Engineering, Mepco Schlenk Engineering College, Tamil Nadu, India
E-mail: [1]s_arivu@yahoo.com, [2]vivimishi@yahoo.co.in, [3]bagavath85@gmail.com

Abstract
Steganographic algorithms in the recent past have been producing stego images with perceptual invisibility, better secrecy and certain robustness against attacks like cropping, filtering etc. Recovering a good quality secret from a good quality stego image may not always be possible. The method proposed in this paper works in transform domain and attempts to extract the secret almost as same as the embedded one maintaining minimal changes to the cover image by using techniques like median maintenance, offset and quantization.

Keywords:
Arnold Transform, Median maintenance, Discrete Wavelet Transform, Improved LSB, Offset, Quantization

1. INTRODUCTION

Steganography literally means *covered writing* as derived from Greek. Steganography is the art of concealing the existence of information within seemingly innocuous carriers. Johnson and Jajodia [1], viewed steganography as akin to cryptography. Both have been used throughout recorded history as means to protect information. At times these two technologies seem to converge while the objectives of the two differ. Cryptographic techniques "scramble" messages so if intercepted, the messages cannot be understood. Steganography, in an essence, "camouflages" a message to hide its existence and make it seem "invisible" thus concealing the fact that a message is being sent altogether. An encrypted message may draw suspicion while an invisible message will not.

Petitcolas *et.al* [2], present a survey on Information hiding showing that such techniques have recently become important in a number of application areas. Digital audio, video and pictures are increasingly furnished with distinguishing but imperceptible marks, which may contain a hidden copyright notice or serial number or even help to prevent unauthorized copying directly. Military communication systems make increasing use of traffic security techniques,which rather than merely concealing the content of a message using encryption, seek to conceal its sender, its receiver or its very existence. Similar techniques are used in some mobile phone systems and schemes proposed for digital elections. Criminals try to use whatever traffic security properties are provided intentionally or otherwise in the available communication systems, and police forces try to restrict their use. However, many of the techniques proposed in this young and rapidly evolving field can trace their history back to antiquity; and many of them are surprisingly easy to circumvent. With high-resolution digital images as carriers, detecting hidden messages has become considerably more difficult.

This paper focuses on colour image steganography. Various techniques have been developed to hide data in digital photographic images. All those techniques can be grouped under two categories, Spatial Domain and Transform Domain techniques.

In Spatial Domain, Least Significant Bit (LSB) based embedding techniques are used most widely because of its ease in implementation. Bassia *et.al* [3], present an audio watermarking using LSB method which produces an output audio signal perceptually similar to original one, but not robust against changes in time domain**.** Rodrigues *et.al* [4], proposed a method, where instead of least significant bits, 4^{th} bit is made use of. In order to minimize the variation in pixel value, the adjacent bits are modified in such a way that the difference between original and modified pixel value is less than 4. Human Visual System (HVS) perception tests show that their results provide good stego images. Lee *et.al* [5] and Cvejic and Seppanen [6] present methods to increase the embedding capacity of LSB based steganography in image and audio respectively. In order to maintain the error difference to be minimal, Minimum Error replacement and Error Diffusion techniques were used. Lee *et.al* [7] made an attempt to embed data adaptively based on the neighbour pixel values. Minimum Error replacement and Error Diffusion were used to reduce error difference. They obtained embedding capacity of the order of 4 bits/pixel. Apart from LSB techniques, Marvel *et.al* [8], present a method, which made use of spread spectrum concept and error control coding for information embedding. Chen and Wornell [9], and Eggers *et.al* [10] proposed methods based on Quantization Index Modulation and Costa schemes for information embedding in spatial domain respectively. Besides embedding, these techniques were also used for authentication application. Mukherjee *et.al* [11], proposed such a method that provides buyer authentication even if attacker tries to manipulate the watermark with the knowledge of the watermarking scheme. Kallel *et.al.* [12], present a two-step based multiple-watermarking scheme in spatial domain for medical images.

Cox *et.al.*[13], present a spread spectrum based watermarking scheme for multimedia objects in transform domain using DCT, which provides good robustness against signal processing operations like lossy compression, filtering, A/D and D/A conversions. Borges *et.al* [14], present a method combining cryptographic techniques like Diffie Hellman, RSA and steganography to provide extreme security. Hovancak *et.al* [15], present a method of information embedding using DWT, where the secret data is pseudo randomly permuted using a secret key. LSB based techniques are also used in transform domain. Cvejic and Seppanen [16], used LSB based technique showing an improvement in embedding capacity by 150-200 kbps of hidden data comparing to spatial domain. As DC coefficients are of higher significance in transform domain, authors like Chen and Lin [17] and Silva and Agaian [18], embed data in insignificant part alone and the latter also made a comparative study using different transforms like DCT, Haar, FFT, Hadamard. Embedding in colour images added another advantage of randomizing embedding of bits among the three colour planes. Kundur and Hatzinakos [19], use such a method in DWT domain. Rongrong and Qiuqi [20], and Yang and Deng [21], make use of this advantage along with chaotic principles to improve robustness, which showed better results.

A detailed study has been made by authors like Bender *et.al* [22], Kharrazi *et.al* [23], and Chan and Cheng [24], where they summarize different types of techniques available for information embedding along with the possible attacks on them and also results were drawn by performing steganalysis on the stego images obtained using those techniques with the available steganalysis methods. It clearly shows that, the methods in spatial domain have larger capacity but weaker robustness, but in transform domain better robustness is achieved. Mythreyi and Vaidehi [25] proposed such a scheme using Gabor transform where they made use of detail bands for embedding which provides a minimal variation in pixel values. Cheddad *et al* [26] present a detailed survey on the state-of-the-art techniques for Steganography and recommends for object oriented Steganography.

In this paper, a modified approach for embedding color images within color images is proposed and it overcomes the limitations in embedding faced by Rongrong and Qiuqi [20]. The rest of this paper is organized as follows. Section 2 gives brief information about the transforms employed in the embedding process. Section 3 represents proposed algorithm, section 4 gives the experimental results and conclusions are drawn in section 5.

2. TRANSFORMS EMPLOYED

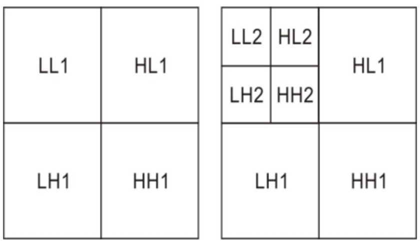
2.1 DISCRETE WAVELET TRANSFORM

On applying Wavelet Transform, the image gets decomposed into four sub bands namely LL1, LH1, HL1 and HH1 as shown in Fig.1 (a). LL1 represents low frequency components, i.e., approximation of the image and the other three refer to the high frequency components, i.e., details of the image.

The decomposition is achieved with a family of real ortho normal bases $\psi_{m,n}(x)$, obtained through translation and dilation of a kernel function ψ (x) known as the mother wavelet, i.e.,

$$\Psi_{m,n}(x) = 2^{-m/2}\,\Psi(2^{-m}x - n) \qquad (1)$$

where, *m* and *n* are integers. To get the next level of wavelet coefficients, the approximation sub band is allowed to undergo further decomposition resulting in two level wavelet decomposition as shown in Fig.1(b). Further decomposition can continue with the resulting approximation bands, till a finer scale is reached as described [27].



(a) (b)

Fig.1. Image Decomposition (a) One-level, (b) Two-level

2.2 ARNOLD TRANSFORM

Arnold transform, also called as cat mapping, changes one matrix into another but of same dimension. Let *A* be a *N x N* matrix, a point *(x, y)* in *A* can be shifted to another point *(x', y')*, given by Eq. (2),

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} (\mathrm{mod}\, N) \qquad (2)$$

After certain number of iterations, matrix *A* reappears. In experimentations, Arnold transformation is performed on secret image and this increases security and robustness of the proposed algorithm. Arnold Transform can provide robustness by avoiding large area information loss of the secret image even though the cover image is cropped [21]. Lou and Sung [28] discuss in detail about chaotic principles.

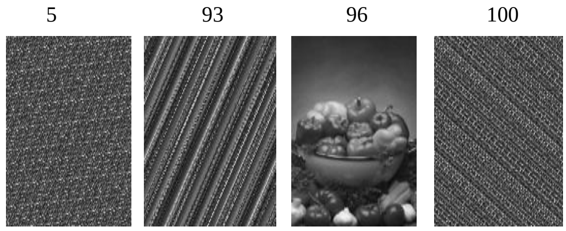


Fig.2. Arnold Transformed Secret at Various Iterations

The Arnold transform applied secret images at various iterations are shown in Fig.2. The original secret image reappears at 96^{th} iteration. The selected iteration to be embedded will be other than the 96^{th} iteration.

3. ALGORITHM

3.1 DATA EMBEDDING

Yang and Deng [21] have used both the cover and secret images as gray level images. Rongrong and Qiuqi [20] proposed a method to hide a gray level secret into a colour cover. Our work aims to hide a colour secret into a colour cover image. Algorithms mentioned by Yang and Deng [21] and Rongrong and Qiuqi [20] are not as such applicable for embedding and extracting colour images because the effects of quantization as well as erroneous extraction are well visible. This work has concentrated to reduce the damage done to the cover image with error free extraction of secret image. The whole embedding process is shown in Fig.3.

The secret image, which is to be embedded, is applied with Arnold Transform to increase the robustness. This transformed data is then split to form the three colour planes namely *R*, *G* and *B*. All the three colour planes are subjected to Discrete Wavelet Transform (DWT) individually. The coefficients of the detail sub bands may also have negative value. The minimum value in each detail sub band is found out and the minimum values are subtracted from corresponding detail sub band coefficient values so that the range of coefficients that need to be embedded now has no negative value. Each plane is then converted to its corresponding bit stream and then concatenated to embed in the cover image. The cover image is also subjected to DWT decomposition after splitting into red, green and blue planes and the coefficient matrix *(C)* is obtained as specified in Eq.(3).

$$C = \begin{Bmatrix} C_{p,l,o}(x,y),\ 0 \le X < N, 0 \le Y < N \\ where,\ p \in \{R,G,B\}, 1 \in \{1,2,3\} 0 \in \{a,h,v,d\} \end{Bmatrix} \quad (3)$$

and *R* ,*G*, *B* denote the colour planes , '*l*' represents levels of decomposition and '*o*' indicates the approximate and detail sub bands.

The secret image bit stream is not embedded uniformly in a single plane of cover image or uniformly across the three colour planes of cover image. The embedding is made random across the three planes, which provide a layer of security to the secret image, and the selection of the plane depends on the cover *R, G*, and *B* plane coefficient values. To embed every single element of the bit stream, one of the coefficients of the transformed cover image, that is the median value of all the three planes considered is selected, i.e., coefficients with the same decomposition level and same sub band part of the cover are sorted down to satisfy the expression given by Eq.(4).

$$C_{p1,l,o}(x,y) \le C_{p2,l,o}(x,y) \le C_{p3,l,o}(x,y) \quad (4)$$
$$where\ p1, p2, p3 \in \{R,G,B\}$$

In both Yang and Deng [21] and Rongrong and Qiuqi [20] model, embedding position is selected in a sequential manner. In the proposed model, the embedding of secret image bit stream in the transformed cover is randomized and hence before the colour plane selection, a random embedding position in the transformed cover will be found out and then colour plane selection will be done at that particular position. This way of randomized embedding provides an additional layer of security to the secret image. The embedding position in the cover is selected by using Eq.(2), which is the one used in Arnold Transform, where (*x, y*) is the embedding position in sequential manner and (*x', y'*) is the corresponding new randomized embedding position and '*N*' is the size of image, *N x N*.

For embedding the approximation sub band of secret into the corresponding counterpart of cover, Improved LSB algorithm is used. Improved LSB algorithm is applied on the selected coefficient with some modifications being introduced. Improved LSB algorithm works on modifying bits around the selected bit position so that the pixel value is closer to that of the original value even after embedding and this ensures that the changes made on the cover is minimal. After the embedding process, the Improved LSB algorithm applied transform coefficient may not remain the median of the three planes and hence causes erroneous data extraction. The proposed algorithm works towards maintaining the median value even after embedding. This helps exact recovery of data for the approximation band.

Regarding the detail sub bands, the embedding algorithm is different. The algorithm is abstracted from Rongrong and Qiuqi [20] model, where after obtaining coefficient matrix specified in Eq.(4), the range of values between $C_{p1,l,o}(x, y)$ and $C_{p3,l,o}(x, y)$ is split down into '*Q*' parts with interval of Δ with alternate dashed and bold lines as shown in Fig.4. To embed bit 0, $C_{p2\ l,\ o}(x, y)$ is modified to the nearest value shown by dashed lines and for 1, bold lines are considered. In Rongrong and Qiuqi [20] model, the main constraint is with the limitation in embedding capacity, as they left positions with Δ value too small as unfit for embedding. Here, those coefficients are also used by increasing and decreasing $C_{p3,l,o}(x, y)$ *and* $C_{p1,l,o}(x, y)$ respectively, with some minimal value. The algorithm followed from Yang and Deng [21] and Rongrong and Qiuqi [20] works well for gray level images but leads to a poor reconstruction of the secret in the extraction phase if directly applied to colour images, as shown in Fig.5(d), (e).

The following are the modifications done to the Yang and Deng [21] and Rongrong and Qiuqi [20] algorithm,

- Using an offset to remove all negative coefficients before embedding and restoring them in the extraction phase
- Randomizing the bit embedding positions before colour plane selection
- Maintaining the median value after embedding in the approximate band and detail bands
- Making use of coefficients which were unfit for embedding in Rongrong and Qiuqi [20] model, by suitable compensation, thereby increasing the embedding capacity

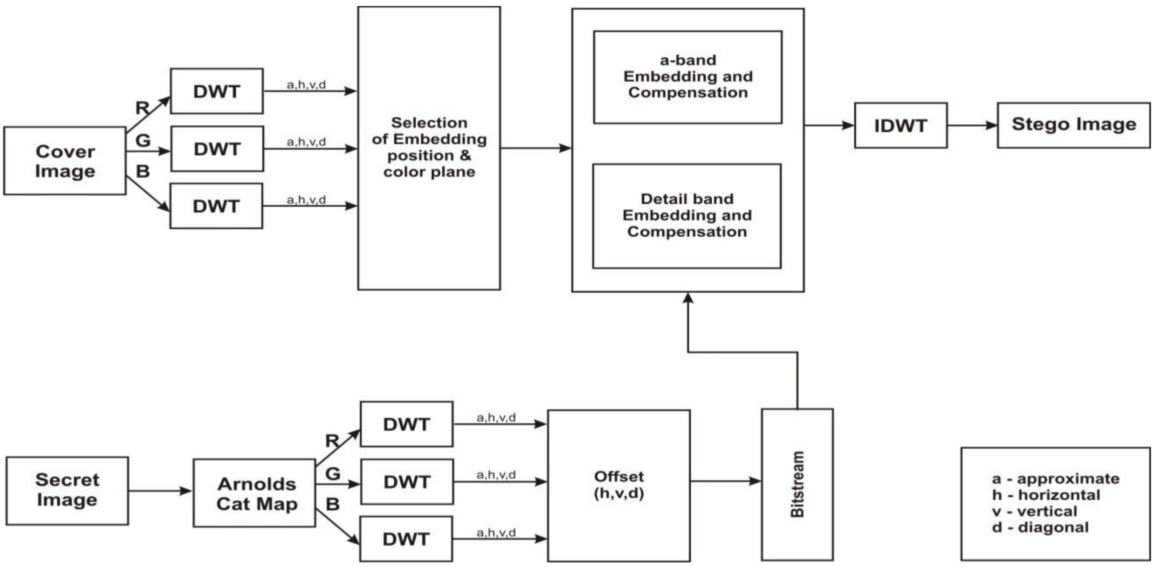


Fig.3. Embedding Process

Once, data embedding is completed, Inverse DWT is applied to each colour plane and then they are concatenated to get a stego image, that contains the secret image with it.

3.2 DATA EXTRACTION

The *R, G* and *B* planes of the received stego image are decomposed by DWT to get coefficient matrix (*C'*). The coefficients with the same decomposition level and sub bands are rearranged in ascending order as specified in Eq. (5).

$$C'_{p1,l,o}(x,y) \le C'_{p2,l,o}(x,y) \le C'_{p3,l,o}(x,y) \quad where\ p1, p2, p3 \in \{R,G,B\} \tag{5}$$

For extracting the approximate sub band of secret image, approximate part is considered in *C'* and coefficients are rearranged as given by Eq.(5) before which the actual embedded position will be found using Eq.(2). The embedded bit is in $C'_{p2,l,o}(x, y)$ and hence i^{th} LSB (bit is being embedded at i^{th} LSB) of $C'_{p2,l,o}(x, y)$ is obtained to get back approximate sub band information of secret.

For extracting the detail sub bands, the range between $C'_{p1,l,o}(x, y)$ and $C'_{p3,l,o}(x, y)$ is split down into '*Q*' equal parts and based on the location of $C'_{p2,l,o}(x, y)$, embedded bit is extracted. As enough compensation works have been done, exact reconstruction is ensured. Once all the sub bands are extracted, offset value present in every transform coefficient is removed followed by application of inverse DWT. Finally required iterations of Arnold Transform are applied to get back the secret Image.

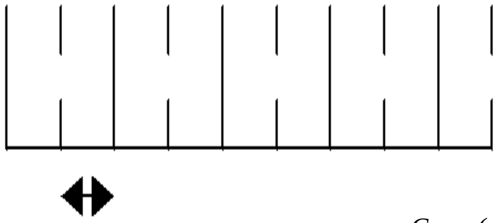
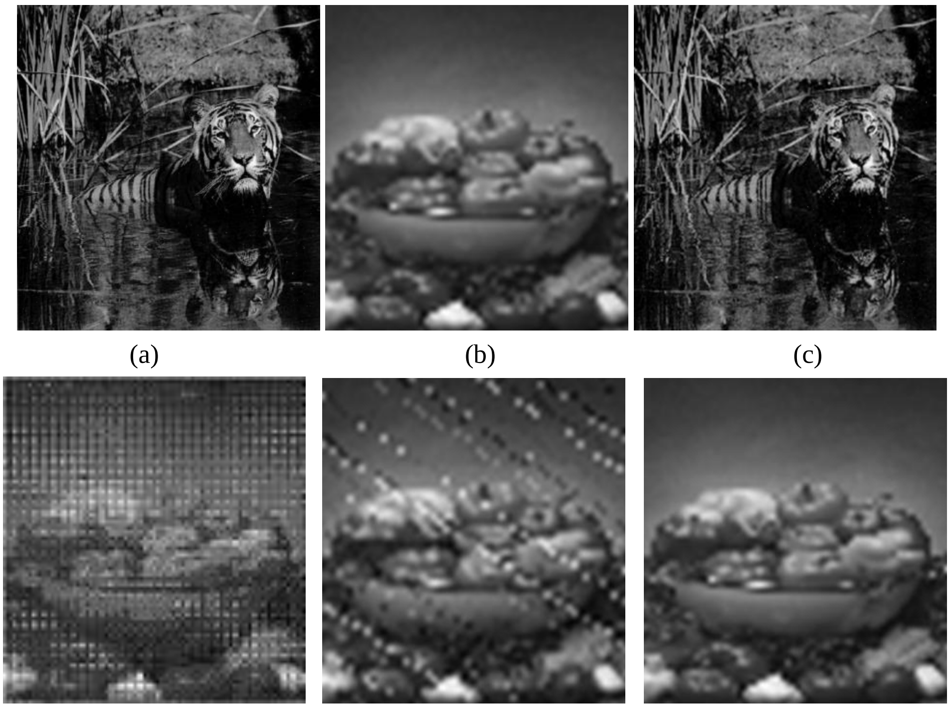


Fig.4. Range Partition

4. EXPERIMENTAL RESULTS AND DISCUSSION

Experimentation is carried out with cover image of size *512 x 512*, and secret image of size *64 x 64*, with *Q=30*, 4^{th} LSB, *3* levels of DWT decomposition and the results are shown in Fig.5. Erroneous extraction of the secret image using Rongrong and Quiqi's method (offset and median are not maintained) is shown in Fig.5(d) and Fig.5(e). Fig.5(f) shows the recovered secret perfectly resembling the original secret, using the proposed method, where offset and median maintenance are performed. For the same cover and secret, the relationship between *Q* and PSNR is shown in Fig 6. Higher the value of *Q*, higher will be PSNR. Also, experimentation is carried out, where the cover and secret images are decomposed up to three levels and it is found that higher PSNR values are obtained at 3^{rd} level of decomposition. Table.1 depicts this relation.



(a) (b) (c)

(d) (e) (f)

Fig.5. Embedding and Recovering of Secret Image: (a) Cover Image (b) Secret Image (c) Stego Image
(d) Recovered secret using Rongrong and Quiqi's method (with no offset)
(e) Recovered secret using Rongrong and Quiqi's method (with no maintenance)
(f) Recovered secret using proposed method (with offset and median maintenance)

Table.1. PSNR and Similarity at different levels of decomposition

Decomposition Levels	1	2	3
PSNR (dB)	48.0321	53.9998	58.9432
Similarity (ρ)	0.999976	0.999984	0.999986

The algorithm has been tested with 50 different images and the secret images were extracted with no error and the PSNR and similarity measures are given in Table.2. For the same 50 images, experimentation is done by embedding secret images of different sizes into cover images of size *512x512*.

It is found that with the reduction of secret image size, the PSNR value gets increased. Fig.7 shows this relation. Also, the same images are decomposed up to 3 levels and embedding is done. The relation between levels of decomposition and PSNR is shown in Fig.8, which clearly indicates that the quality of the stego image gets better with embedding done at sub bands of a higher level decomposition. A comparison has been done between the PSNR values obtained using randomized embedding and sequential embedding and it is shown in Fig.9. Results clearly reveal that on the whole PSNR is not affected and randomized embedding even shows improvement in PSNR for some images.

For comparing the results, the same set of images have been subjected to Rongrong and Quiqi's method as well as Yang and Deng's method. As evident from Table.2, though all the methods have comparable PSNR values, the similarity measure nearly equals unity in the proposed method owing to median maintenance. Implementing Yang and Deng's method, the same embedding algorithm has been used for all the four sub bands. The other implementation is different in the way that it has Improved LSB algorithm for the approximation band.

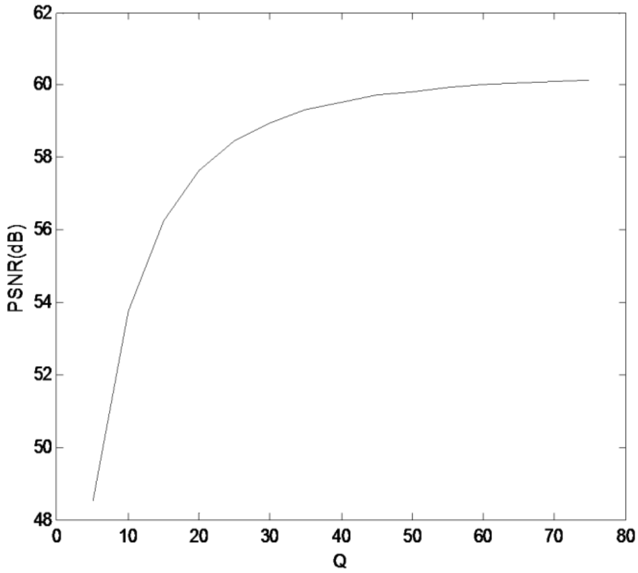


Fig.6. Relation between Q and PSNR

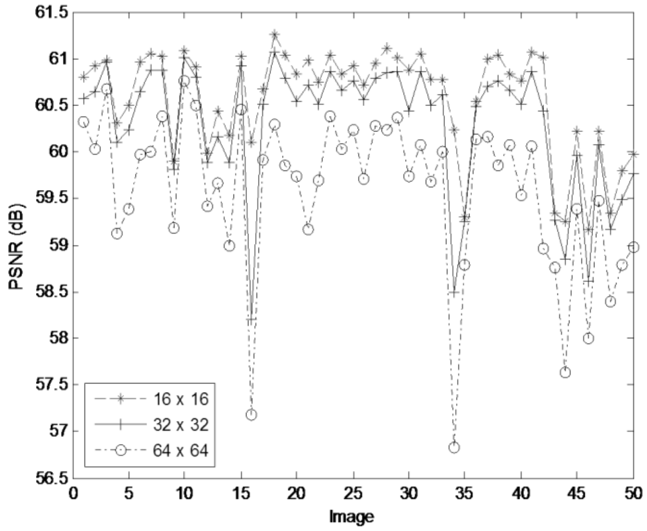


Fig.7. PSNR for 50 different Stego Images Embedded with different Secret Image sizes

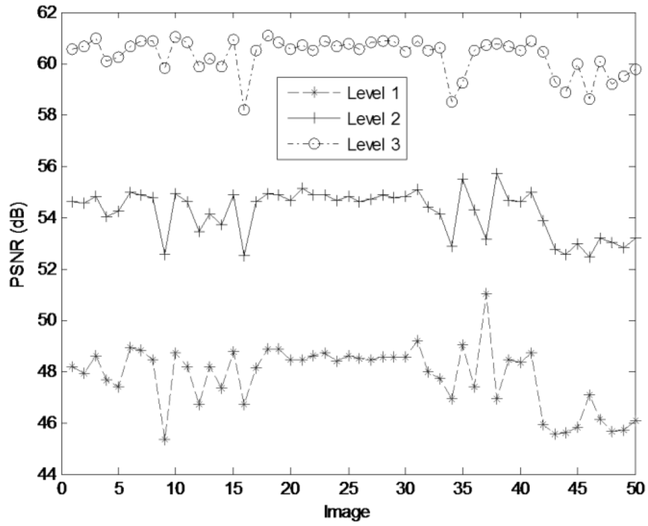


Fig.8. PSNR at Different Levels of Decomposition of cover and Secret

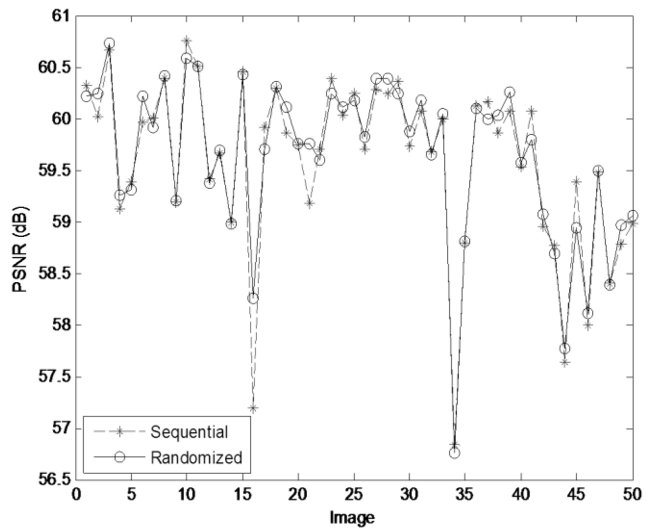


Fig.9. PSNR for Randomized and Sequential Embedding

In order to justify the results obtained using the proposed algorithm, the obtained results are also compared with the results obtained using some commercially available steganographic software. Two such software is,

1. Invisible secret's 4.6
2. Puff V 1.1

Experimentation is carried out using the 50 Image Database with cover images of size 512 x 512 and secret images of size 32 x 32 for both the software. Fig.10 and Fig.11 depict the significance of the proposed algorithm delivering higher PSNR values than Invisible Secret's and Puff V 1.1 respectively.

Peak Signal to Noise ratio (PSNR) is computed using,

$$PSNR = 10\log_{10}\frac{255^2}{MSE}\ dB \tag{6}$$

$$MSE = \left(\frac{1}{N^2}\right)\sum_{1}^{N-1}\sum_{1}^{N-1}\left(\alpha_{x,y} - \beta_{x,y}\right)^2$$

where, MSE represents Mean Square Error and $\alpha_{x,y}$, $\beta_{x,y}$ are pixel value of the cover and stego images respectively.

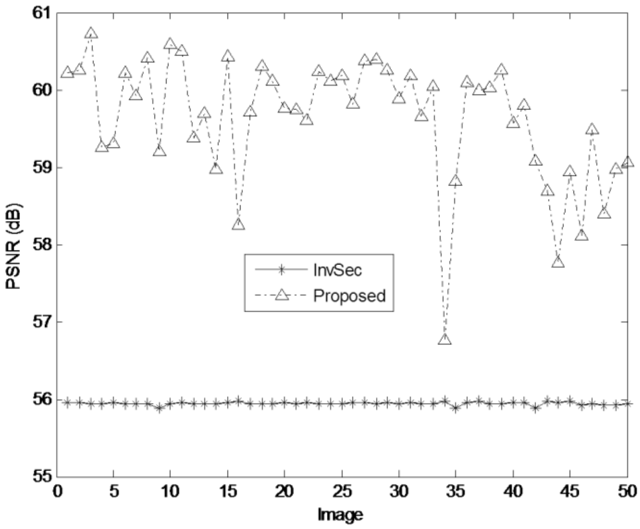


Fig.10. PSNR of Proposed Algorithm vs Invisible Secret's 4.6

Table.2. PSNR and Similarity measures for 50 different Images

Cover / Secret (512 x 512) / (64 x 64)													
Image	PSNR (dB)			SIMILARITY (ρ)			Image	PSNR (dB)			SIMILARITY (ρ)		
	Yang and Deng Method	Rongrong and Qiuqi Method	Proposed Method	Yang and Deng Method	Rongrong and Qiuqi Method	Proposed Method		Yang and Deng Method	Rongrong and Qiuqi Method	Proposed Method	Yang and Deng Method	Rongrong and Qiuqi Method	Proposed Method
1	60.66083	60.2680	60.21078	0.819441	0.8081	0.999987	26	62.43028	59.7701	59.81595	0.835496	0.8737	0.999994
2	59.77698	60.2888	60.24843	0.853535	0.9295	0.999993	27	63.99200	60.3118	60.38264	0.785417	0.7560	0.999984
3	64.94084	60.6582	60.72924	0.816851	0.7971	0.999987	28	59.72597	60.3909	60.39295	0.841767	0.8074	0.999977
4	64.07962	59.2494	59.26282	0.862596	0.8904	0.999988	29	63.94363	60.3090	60.24893	0.846248	0.8512	0.999989
5	64.26044	59.3607	59.30282	0.868358	0.9062	0.999992	30	62.69742	59.8254	59.87912	0.863345	0.8681	0.999988
6	55.79221	60.1663	60.21974	0.844437	0.8795	0.999992	31	52.79631	60.1879	60.18104	0.848513	0.8236	0.999988
7	53.85821	59.9028	59.91817	0.881903	0.8832	0.999988	32	63.50434	59.6839	59.65775	0.828423	0.8009	0.999976
8	55.97786	60.3455	60.41597	0.838184	0.8734	0.999994	33	65.70772	60.0437	60.04651	0.84405	0.8205	0.999991
9	65.85572	59.1241	59.19956	0.801033	0.7728	0.999987	34	65.38603	56.7810	56.76296	0.856197	0.8853	0.999988
10	59.70899	60.6345	60.587	0.816672	0.7716	0.999976	35	59.21595	58.7901	58.80748	0.799195	0.7927	0.999986
11	62.09432	60.4883	60.50399	0.850893	0.8177	0.999989	36	64.65303	60.0682	60.09628	0.844491	0.8709	0.999989
12	61.77921	59.4329	59.37091	0.838363	0.8413	0.999977	37	58.93425	60.0211	59.99739	0.783605	0.7547	0.999978
13	63.45463	59.7498	59.68549	0.856446	0.8658	0.999987	38	59.15379	60.0295	60.02663	0.863677	0.9134	0.999992
14	64.71031	58.9498	58.97768	0.838004	0.8384	0.999986	39	64.38753	60.2746	60.25577	0.847336	0.8832	0.999993
15	62.36098	60.3925	60.42421	0.849254	0.9247	0.999994	40	62.84414	59.5641	59.56595	0.87203	0.9492	0.999994
16	58.83114	58.1848	58.25599	0.864449	0.8879	0.99999	41	55.53627	59.8658	59.79923	0.877489	0.9714	0.999998
17	61.7279	59.7969	59.70514	0.80497	0.7619	0.999958	42	61.39092	59.0627	59.07706	0.823376	0.8066	0.999989
18	57.54989	60.2588	60.30751	0.876532	0.8650	0.999988	43	58.54912	58.7006	58.68989	0.875094	0.9740	0.999998
19	55.4927	60.0619	60.10596	0.854195	0.8243	0.999983	44	61.64844	57.7382	57.77051	0.885175	0.9337	0.999993
20	58.39934	59.7161	59.75687	0.830376	0.8289	0.999992	45	64.05532	60.0923	58.9437	0.905949	0.9956	0.999997
21	47.87059	59.7823	59.75259	0.847221	0.8346	0.999986	46	63.65717	58.0079	58.10647	0.892977	0.9972	0.999997
22	60.43995	59.6922	59.60491	0.855854	0.8623	0.999991	47	59.41988	59.4860	59.48861	0.784549	0.7656	0.999977
23	59.21529	60.2520	60.24167	0.863457	0.8509	0.999984	48	62.75822	58.3425	58.39313	0.812118	0.8012	0.999988
24	62.93562	60.0637	60.11253	0.828968	0.8391	0.999984	49	61.78266	58.9424	58.96843	0.788061	0.7642	0.99998
25	59.37844	60.3201	60.17862	0.839657	0.7945	0.999967	50	58.8775	58.9870	59.06023	0.813073	0.7980	0.999947

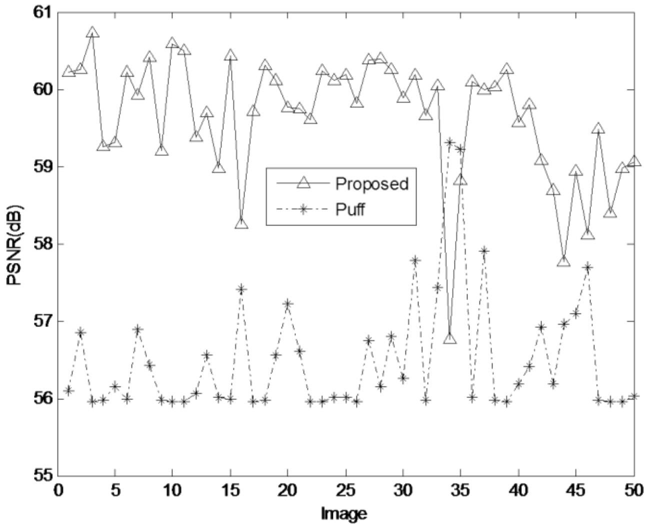


Fig.11. PSNR of Proposed Algorithm vs Puff V.1.1

The similarity between original embedded secret and recovered secret is given by,

$$\rho = \frac{\sum\sum SS^{'}}{\left(\sum S^{2}\right)^{1/2}\left(\sum S^{'2}\right)^{1/2}} \quad (7)$$

where, 'S' is the original secret image and 'S'' is the recovered secret image.

5. CONCLUSION

This paper presents an algorithm that embeds a colour secret image into a colour cover image at transformed level. The random selection of embedding position and distribution of secret data among *R*, *G*, and *B* planes of the cover image increases the security of the secret. The permutation of secret image increases the robustness and the absence of cover image for extraction is yet another advantage. From Table.2, it is evident that using the proposed method the secret images are extracted almost as same as the embedded original image with minimal changes to the cover image.

REFERENCES

[1] N.F. Johnson and S. Jajodia, "Exploring Steganography: Seeing the Unseen", *IEEE Computer*, Vol. 31, No. 2, pp. 26-34, 1998.

[2] F.A. Petitcolas, A.J. Anderson and M.G. Kuhn, "Information Hiding –A Survey", *Proceedings of the IEEE, Special Issue on Protection of Multimedia Content*, Vol. 87, No. 7, pp.1062-1078, 1999.

[3] P. Bassia, I. Pitas and N. Nikolaidis, "Robust Audio Watermarking in Time Domain", *IEEE Transaction on Multimedia*, Vol. 3, No. 2, pp.232-241, 2001.

[4] J.M. Rodrigues, J.R. Rios and W. Puech, "SSB-4 System of Steganography Using bit 4", *5th International Workshop on Image Analysis for Multimedia Interactive Services, Portugal*, 2004.

[5] Lee, Y.K and L.H. Chen, "High Capacity Image Steganographic model", IEE Proceedings on Vision, Image and Signal Processing, Vol. 147, No. 3, pp. 288-294, 2000.

[6] N. Cvejic and T. Seppanen, "Increasing the Capacity of LSB based Audio Steganography", *IEEE workshop on Multimedia Signal Processing*, pp. 336-338, 2002.

[7] Lee, Y.Kwen and L.H.Chen.L.H, "An Adaptive Image Steganographic Model Based on Minimum-Error LSB Replacement", *Ninth National Conference on Information Security*, pp. 8-15, 1999.

[8] L.M. Marvel, C.G. Boncelet and Jr.C.T. Retter, "Spread Spectrum Image Steganography", *IEEE Transaction on Image Processing*, Vol. 8, No. 8, 1999.

[9] B. Chen and G.W. Wornell, "Quantization Index Modulation: A Class of provably Good Methods for Digital Watermarking and Information Embedding", *IEEE Transaction on Information Theory*, Vol. 47, No. 4, pp.1423-1443, 2001.

[10] J.J. Eggers, R. Bauml, R. Tzschoppe and B. Girod, "Scalar Costa Scheme for Information Embedding", IEEE Transactions on Signal Processing, Vol. 51, No. 4, pp. 1003 – 1019, 2003.

[11] D.P. Mukherjee, S. Maitra and S.T. Acton, "Spatial Domain Digital Watermarking of Multimedia Objects for Buyer Authentication", *IEEE Transactions on Multimedia*, Vol. 6, No. 1, pp. 1-15, 2004.

[12] M. Kallel, J.C. Lapayre and M.S. Bouhlel, "A Multiple Watermarking Scheme for Medical Image in Spatial Domain", International Journal on Graphics, Vision and Image Processing, Vol. 7, No. 1, pp. 37-42, 2007.

[13] I.J. Cox, J. Killian, F.T. Leighton and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia", *IEEE Transactions on Image Processing*, Vol. 6, No. 12, pp. 1673-1687, 1997.

[14] F. Borges, R. Portuga and J. Oliveria, "Steganography with Public Key Cryptography for Video Conferencing", *CNMAC*, 2007, www.lncc.br/~borges/doc.

[15] R. Hovancak, P. Foris and D. Levicky, "Steganography Based on DWT Transform", Radioelektronika, 2006, http://www.urel.feec.vutbr.cz/ra2007/archive/ra2006.

[16] N. Cvejic and T. Seppanen, "A Wavelet Domain LSB Insertion Algorithm for High Capacity Audio Steganography", *Proceedings of 10th IEEE Digital Signal Processing Workshop*, pp. 53-55, 2002.

[17] P.Y. Chen and H.J. Lin, "A DWT Based Approach for Image Steganography", *International Journal of Applied Science and Engineering*, Vol. 4, No. 3, pp. 275-290, 2006.

[18] E.A. Silva and S.S. Agaian, "The Best Transform in the Replacement Coefficients and the Size of the Payload Relationship Sense", *Proceedings of the Society for Imaging Science and Technology*, pp. 199-203, 2004.

[19] D. Kundur and D. Hatzinakos, "Digital Watermarking Using Multiresolution Wavelet Decomposition", *Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing*, Vol. 5, pp. 2969-2972, 1998.

[20] N. Rongrong and R. Qiuqi, "Embedding Information into Color Images Using Wavelet", *Proceedings of IEEE Region 10 Conference on Computers, Communications, Control and Power Engineering*, Vol. 1, pp. 598-601, 2002.

[21] B. Yang and B. Deng, "Steganography in Gray Images Using Wavelet", Proceedings of the second International symposium on Communication, Control and Signal Processing, 2006.

[22] W. Bender, D. Gruhl and N. Morimoto, "Techniques for Data Hiding", *IBM Systems Journal*, Vol. 35, No. 3.4, pp. 313-336, 1996.

[23] M. Kharrazi and H.K. Sencar, "Performance Study of Common Image Steganography and Steganalysis Techniques", *Journal of Electronic Imaging*, Vol. 15, No.4, 2006.

[24] C.S. Chan and C.C. Chang, "A Survey of Information Hiding Schemes for Digital Images", *International Journal of Computer Sciences and Engineering Systems*, Vol. 1, No. 3, pp. 187-200, 2007.

[25] Mythreyi and Vaidehi, "Gabor Transform Based Image Steganography", *IETE Journal of Research*, Vol. 53, No. 2, pp. 103-112, 2007.

[26] Abbas Cheddad, Joan Condell, Kevin Curran and Paul Mc Kevitt, "Digital image Steganography: Survey and analysis of current methods", *Signal Processing*, Vol. 90, No. 3, pp. 727-752, 2010.

[27] S.G. Mallat, "A Theory for Multiresolution Signal Decomposition: The Wavelet Representation", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 11, No. 7, pp. 674-693, 1989.

[28] D.C. Lou and C.H. Sung, "A Steganographic Scheme for Secure Communications Based on The Chaos and Euler Theorem", *IEEE Transactions on Multimedia*, Vol. 6, No. 3, 2004.