http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet

Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 11 (5): 587-595, 2012
ISSN 1812-5638 / DOI: 10.3923/itj.2012.587.595

Inverted Pattern in Inverted Time Domain for Icon Steganography

Rengarajan Amirtharajan and John Bosco Balaguru Rayappan
Department of Electronics and Communication Engineering,
School of Electrical and Electronics Engineering, SASTRA University,
Thanjavur, 613401, India

Abstract: Information technologies and communications have pervaded our homes and business places. No matter how well-organized and extensive the communication technology is there are always loop holes in the network and people who seek after the clandestine information to extract from these loop holes. The pandemic problem of security is still a raging problem as every solution compromises on one trait to heighten the other(s) according to the necessity of the hour. In this paper we suggest an algorithm where we have tried to retain all the three important banalities of secure communication: robustness, capacity and imperceptibility by using Haar Integer wavelet transform a Discrete Wavelet Transform (DWT) domain method in tandem with a cryptic scheme i.e. the direct binary or inverted binary embedding of data. Experimental results that compute the MSE and PSNR show that this algorithm caters to the need of the hour by delivering the high capacity with good imperceptibility.

Key words: Information hiding, steganography, integer wavelet transform, inverted pattern

INTRODUCTION

In this age of booming communication and technology, everything is just one phone call or e mail or a flight away. The free flow of information has behooved the need for protecting this huge wealth of knowledge that has from time to time helped tremendously in growth of science, technologies, civilizations and mankind as a whole. With the invention of various algorithms for intelligent storing, processing and transmitting of information ranging from minutiae procedures to long exhaustive routines, many techniques have been developed for computer security, information security and information assurance. The most prominent amongst them is steganography (Stefan and Fabin, 2000, Petitcolas *et al*., 1999; Rabah, 2004; Cheddad *et al*., 2010). It involves communicating secret data in an appropriate multimedia carrier (Bender *et al*., 1996; Rabah, 2004), e.g., image (Hmood *et al*., 2010a; Amirtharajan and Balaguru, 2009; Amirtharajan *et al*., 2011), audio (Zhu *et al*., 2011), video (Al-Frajat *et al*., 2010) and text files (Al-Azawi and Fadhil, 2010; Yang *et al*., 2011; Shirali-Shahreza and Shirali-Shahreza, 2008).

Cryptography another popular technique for information security involves scrambling of data in an unintended format which would seem gibberish to any unintended user (Schneier, 2007). No extraction can be done unless the third party knows the secret code. However, it would invite tampering just because of the existence of a secret message. That's where steganography has gained its impetus, with its basic constituents being a cover image, secret data and a key (Stefan and Fabin, 2000; Petitcolas *et al*., 1999; Rabah, 2004). The basic differences between cryptography and steganography is given by Zaidan *et al*. (2010) and Cheddad *et al*. (2010). When combined it gives out a stego image which has high un-detectability, is robust and also has high capacity (Hmood *et al*., 2010b) fulfilling requirements of the "Fridrich's magic Triangle" in information hiding (Stefan and Fabin, 2000; Padmaa *et al*., 2011). Any files such as audio, video or image can be used as cover (Bender *et al*., 1996; Rabah, 2004), cover being the carrier without secret data in it, after embedding secret data in the cover; it is camouflaged with high level of imperceptibility and dexterity to yield the stego image. Here capacity or payload would mean the total amount of secret information that can be hidden in the stego image, without any physical notice-ability in the characteristics of the cover image while robustness defines the limit of standing modifications before an adversary can destroy the stego image. Within steganography, there are various techniques or methods to embed the data in the cover

Corresponding Author: Rengarajan Amirtharajan, Department of Electronics and Communication Engineering, School of Electrical and Electronics Engineering, SASTRA University, Thanjavur, 613401, India

image i.e., Substitution based (Amirtharajan and Balaguru, 2009; Chan and Cheng, 2004), Transform domain based (Thanikaiselvan *et al*., 2011a), Spread Spectrum based (Amirtharajan and Balaguru, 2011; Thenmozhi *et al*., 2011; Kumar *et al*., 2011), Statistics based (Qin *et al*., 2009; Zanganeh and Ibrahim, 2011), Distortion and cover generation based (Xiang *et al*., 2011; Stefan and Fabin, 2000).

The most prominent being Spatial Domain based Steganographic Techniques and Transform Domain based Steganographic Techniques (Thanikaiselvan *et al*., 2011a; Kumar *et al*., 2011), Spatial domain based steganography include the Least Significant Bit (LSB) technique (Amirtharajan and Balaguru, 2009; Chan and Cheng, 2004), Pixel value differencing (Amirtharajan *et al*., 2010; Thanikaiselvan *et al*., 2011b; Padmaa *et al*., 2011) and more while the latter includes DCT (Provos and Honeyman, 2003), DWT and especially IWT (Thanikaiselvan *et al*., 2011a; El Safy *et al*., 2009). A detailed survey on steganography till 1999 is available in Petitcolas *et al*. (1999) whereas a detailed survey on Information hiding in images, differences among cryptography, Steganography (Zaidan *et al*., 2010) and water marking is available Cheddad *et al*. (2010). The counter attack called steganalysis is described by Qin *et al*. (2009) and Xia *et al*. (2009) and various steganalysis review is detailed by Qin *et al*. (2010).

A steganography technique is considered to be dependable when it can retain the embedded data in spite of severe modifications done to it and not displaying the payload contained in it. The most employed technique for this involves transforming the cover image into another domain and embedding data in the transformed pixels (Thanikaiselvan *et al*., 2011a; El Safy *et al*., 2009). Before transformation the cover image exists in spatial domain, which is transformed into the frequency or time domain for the coefficients and after embedding data in the transformed pixels, it is brought back to the spatial domain. Thus, the underlying idea is, even if image is subjected to modifications and is in worst cases transformed, the data will still be hidden in the transformed pixels (Thanikaiselvan *et al*., 2011a).

Transformation techniques include DCT, DWT and IWT, though DCT isn't highly preferred as it has low hiding capacity (Provos and Honeyman, 2003). Contemporary researchers use DWT, since it can be employed in compression of formats JPEG2000 and MPEG4. Techniques that use DWT i.e., wavelet transform based stego technique provides high capacity with the secret message embedded into the high frequency and low frequency coefficients of the wavelet transform, but provides less PSNR at a high hiding rate.

Cryptography in coalesce with steganography either through random walk (Luo *et al*., 2008) or variable bit optimal embedding (Zanganeh and Ibrahim, 2011) could be an effective solution to improve the complexity. In this study we propose a new modified version of the methodology by Thanikaiselvan *et al*. (2011a) which can embed a larger amount of data in Integer Wavelet Transform (IWT) domain with high PSNR while combining with the inverted pattern approach (Yang, 2008; Amirtharajan and Rayappan, 2012) to improve the complexity.

Related works: The use of Wavelet transform will mainly address the capacity and robustness of the information-hiding system features. The Haar Wavelet Transform is the simplest of all wavelet transform. In this the low frequency wavelet coefficients are generated by averaging the two pixel values and high frequency coefficients that are generated by taking half of the difference of the same two pixels (El Safy *et al*., 2009). The four bands obtained are LL, LH, HL and HH which is shown in Fig. 1. The LL band is called as approximation band which consists of low frequency wavelet coefficients and contains significant part of the spatial domain image. The other bands are called as detail bands which consist of high frequency coefficients and contain the edge details of the spatial domain image.

Integer wavelet transform: Integer wavelet transform can be obtained through lifting scheme. Lifting scheme is a technique to convert DWT coefficients to Integer coefficients without losing information.

Forward Lifting scheme in IWT:

Step 1: Column wise processing to get H and L:

$$H = (Co-Ce) \quad (1)$$

$$L = (Ce-[H/2]) \quad (2)$$

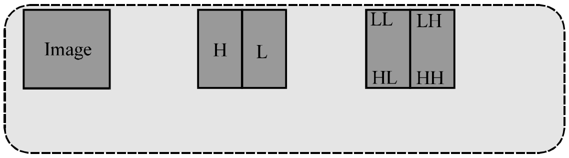

Fig. 1: Image and its transform domain bands

Where, Co and Ce is the odd column and even column wise pixel values

Step 2: Row wise processing to get LL, LH, HL and HH, Separate odd and even rows of H and L, Namely

$$LH = L_{odd}\text{-}L_{even} \tag{3}$$

$$LL = L_{even}\text{-}\lfloor LH/2 \rfloor \tag{4}$$

$$HL = H_{odd}Heven \tag{5}$$

$$HH = H_{even}\text{-}\lfloor HL/2 \rfloor \tag{6}$$

Where:

H_{odd} = Odd row of H
L_{odd} = Odd row of L
H_{even} = Even row of H
L_{even} = Even row of L

Reverse lifting scheme in IWT: Inverse Integer wavelet transform is formed by Reverse lifting scheme. Procedure is similar to the forward lifting scheme (Thanikaiselvan *et al*., 2011a; EI Safy *et al*., 2009).

LSB Embedding: Simple LSB embedding is detailed by Amirtharajan and Balaguru (2009), Chan and Cheng (2004) and Janakiraman *et al.* (2012). Consider a 8-bit gray scale image matrix consisting m×n pixels and a secret message consisting of k bits. The first bit of message is embedded into the LSB of the first pixel and the second bit of message is embedded into the second pixel and so on. The resultant stego-image which holds the secret message is also a 8-bit gray scale image and difference between the cover image and the stego-image is not visually perceptible. This can be further extended and any number of LSB's can be modified in a pixel. The quality of the image, however degrades with the increase in number of LSB's. Usually up to 4 LSB's can be modified without significant degradation in the message. Mathematically, the pixel value 'P' of the chosen pixel for storing the k-bit message Mk is modified to form the stego-pixel 'Ps' as follows:

$$Ps = P\text{-mod}\ (P,2^k)\text{+}Mk \tag{7}$$

The embedded message bits can be recovered by:

$$Mk = \text{mod}\ (Ps,2^k) \tag{8}$$

One method to improve the quality of the LSB substitution is Optimal Pixel adjustment Process (OPAP) (Chan and Cheng, 2004).

Determination of embedding:

- Direct Binary embedding of data is done and the MSE (Mean Square Error) calculated
- Let it assumed to be X
- Inverted Binary embedding of data is done and the MSE (Mean Square Error) calculated
- Let it assumed to be Y
- Depending upon values of X and Y, If X > Y
- Then the value is determined to be '1' and if Y > X
- Then the value is determined to be '0'

PROPOSED METHODOLOGY

The proposed block diagram of high capacity steganography system is given in Fig. 2 and 3. Preprocessing includes R, G and B plane separation and Histogram modification. Then Integer wavelet transform is applied to the cover image to get wavelet coefficients. Wavelet coefficients are randomly selected by using key-2 for embedding the secret data. Key -2 is 8×8 binary matrix in which '1' represents data embedded in the corresponding wavelet coefficients and '0' represents no data present in the wavelet coefficients. Then the direct binary or inverted binary embedding of data is done in the respective co-efficient. Key-1(K1) is a decimal number varying from 1 to 4 and it will decide the number of bits to be embedded in the cover object. High capacity is achieved by varying the key-1 (K1) value.

Embedding Algorithm

Step 1: The cover image of size 256×256×3 pixels is selected
Step 2: The respective planes are separated into R, G and B constituents
Step 3: The required data file to be embedded is taken with each character taking 8 bits
Step 4: Histogram modification is done in all planes, Because, the secret data is to be embedded in all the planes, while embedding integer wavelet coefficients produce stego-image pixel values greater than 255 or lesser than 0. Then all the pixel values will be ranged from 15 to 240
Step 5: Each plane is divided into 8×8 blocks
Step 6: Apply Haar Integer wavelet transform to 8×8 blocks of all the planes, this process results in LL1, LH1, HL1 and HH1 sub bands
Step 7: Using Key-1(K1) calculate the Bit length (BL) for corresponding wavelet co-efficients (WC), here we used modified version of Bit length calculation used by Thanikaiselvan *et al.* (2011a). Using the following equation, we get the high capacity steganography

$$BL=\begin{cases} K1+3 \ \text{if}\ WC \geq 2^{K1+2} \\ K1+1 \ \ \text{if}\ WC < 2^{K1+2} \end{cases} \tag{9}$$

Step 8: Using key-2 select the position and coefficients for embedding the 'BL' length data using LSB substitution. Here data is embedded only in LH1, HL1and HH1 subbands. Data is not embedded in LL1 because they are highly sensitive and also to maintain good visual quality after embedding data. An example of key-2 is shown below (This is Key B)

$$\text{key}-2=\begin{bmatrix}0&0&0&0&1&0&1&0\\0&0&0&0&0&1&0&1\\0&0&0&0&1&0&1&0\\0&0&0&0&0&1&0&1\\1&1&1&1&0&1&0&1\\1&1&1&1&1&0&1&0\\1&1&1&1&0&1&0&1\\1&1&1&1&1&0&1&0\end{bmatrix}- \qquad (10)$$

Step 10: After doing required operations with K-1 and K-2, the direct binary embedding of required data is done in the determine position and co-efficient and MSE calculated

Step 11: Next inverted binary embedding of the same data is done in the same position and corresponding MSE calculated

Step 12: Depending upon MSE values obtained Key-3 (K-3) is obtained with value '1' when inverted binary is embedded and '0' when direct binary is embedded. Thus K-3 is also an 8*8 matrix consisting of 1s and 0s representing whether direct or inverted binary embedding of data is done

Step 13: Applying Optimal Pixel adjustment Procedure (OPAP) reduces the error caused by the LSB substitution method

Step 14: Take inverse wavelet transform to each 8×8 block and combine R,G&B plane to produce stego image

Extraction Algorithm

Step 1: The corresponding stego image of 256*256 pixels is selected

Step 2: The respective planes are separated into R, G and B constituents

Step 3: Each plane is divided into 8×8 blocks

Step 4: Apply Haar Integer wavelet transform to 8×8 blocks of all the planes, This process results LL1,LH1, HL1 and HH1 sub-bands

Step 5: Using Key-1 calculate the Bit length(BL) for corresponding wavelet co-efficients(WC), using the 'BL' equation used in Embedding procedure

Step 6: Using key-2 select the position and coefficients for extracting the 'BL' length data

Step 7: Then using key-3, determine whether direct or inverted binary of the data has been embedded and extract it then depending upon it

Step 8: Combine all the bits and divide it in to 8 bits to get the text message

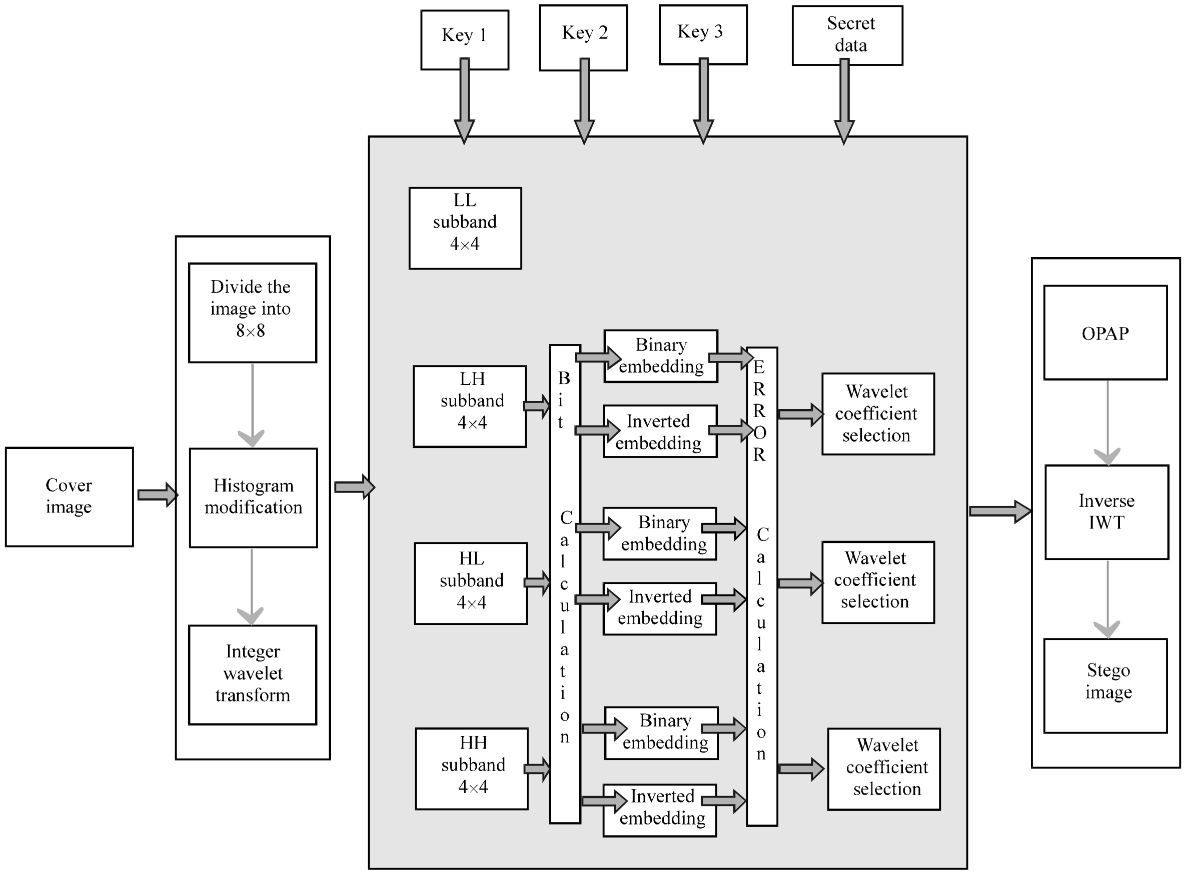

Fig. 2: Block diagram for Embedding

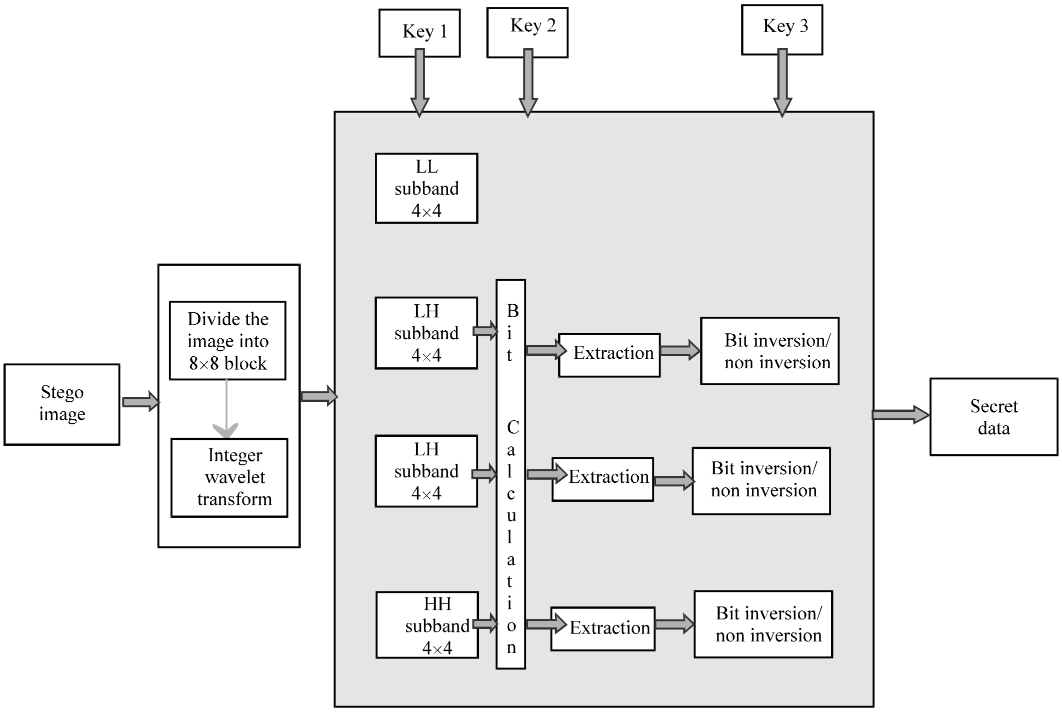
Key 1
Key 2
Key 3
Stego image
Divide the image into 8×8 block
Integer wavelet transform
LL subband 4×4
LH subband 4×4
LH subband 4×4
HH subband 4×4
Bit Calculation
Extraction
Extraction
Extraction
Bit inversion/ non inversion
Bit inversion/ non inversion
Bit inversion/ non inversion
Secret data

Fig. 3: Block diagram for extraction

ERROR METRICS

A performance measure in the stego image is measured by means of two parameters namely, Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR). The MSE is calculated by using the equation:

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(X_{i,j} - Y_{i,j})^2 \qquad (11)$$

where, M and N denote the total number of pixels in the horizontal and the vertical dimensions of the image $X_{i,\ j}$ represents the pixels in the original image and $Y_{i,\ j}$, represents the pixels of the stego-image. The Peak Signal to Noise Ratio (PSNR) is expressed as:

$$PSNR = 10\log_{10}\left(\frac{I_{max}^2}{MSE}\right)dB \qquad (12)$$

RESULTS AND DISCUSSION

In this present implementation, Lena and baboon 256×256×3 color digital images have been taken as cover images, as shown in Fig. 4a and 5a, Stego lena (Thanikaiselvan *et al*., 2011a) in Fig. 4b and 5b and Proposed Stego images in Fig. 4c and 5c and tested with key-1(key-J) and various key-2s. The effectiveness of the stego process proposed has been studied by calculating MSE and PSNR for the Lena and Baboon digital image in RGB planes and tabulated.

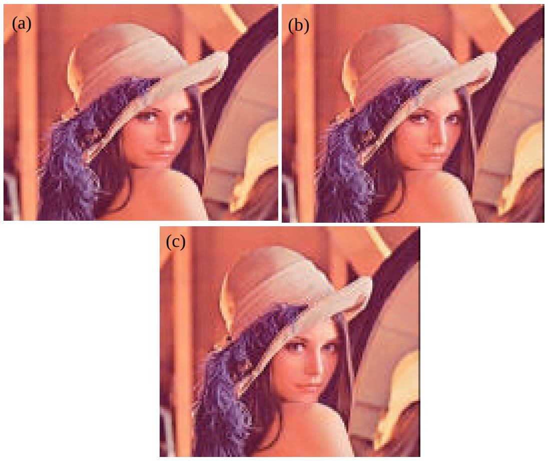

Fig. 4(a-c): (a) Cover Images Lena; (b) Stego lena (Thanikaiselvan *et al.*, 2011a); (c) Proposed Stego lena

In this analysis, Key-2 is used for random selection of coefficients for embedding data (in this analysis Key-1 has been set as K1 = 1) and the results are tabulated in

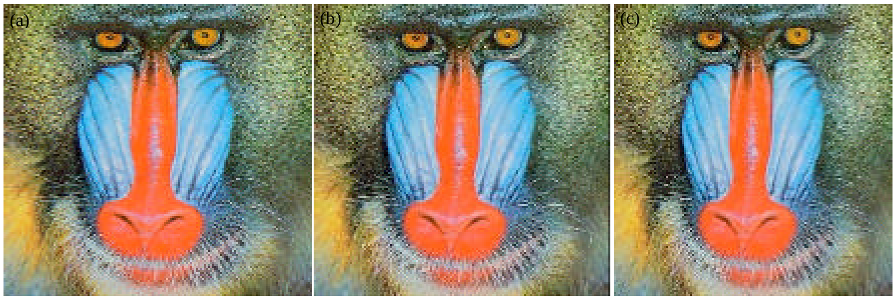

Fig. 5(a-c): (a) Cover Images Baboon; (b) Stego Baboon (Thanikaiselvan *et al*., 2011a); (c) Proposed Stego Baboon

Table 1: Comparative Analysis for the proposed method key - 1(K1) = 1

			Channel - I Red		Channel - II Green		Channel - III Blue	
Various key -1	Cover image	Total No. of bits embedded	MSE	PSNR	MSE	PSNR	MSE	PSNR
Key - A	Lena*	52345	1.3495	46.82	0.7531	49.36	0.4904	51.22
	Lena	52345	1.2166	47.28	0.6033	50.32	0.3399	52.81
	Baboon*	94061	2.7146	43.79	1.8565	45.4438	2.2742	44.5624
	Baboon	94061	2.2419	44.62	1.4034	46.659	1.8155	45.5408
Key - B	Lena*	63138	1.6245	46.02	1.0736	47.82	0.7534	49.36
	Lena	63138	1.4084	46.64	0.8472	48.85	0.5325	50.86
	Baboon*	92959	2.5767	44.02	1.7415	45.7215	2.2435	44.6215
	Baboon	92959	2.1293	44.84	1.3098	46.9588	1.7743	45.6405
Key - C	Lena*	53951	1.0511	47.91	0.4232	51.86	0.1797	55.58
	Lena	53951	1.0483	47.92	0.4162	51.938	0.1745	55.71
	Baboon*	105293	1.4987	46.37	0.631	50.1304	1.076	47.8128
	Baboon	105293	1.4862	46.41	0.6269	50.159	1.0553	47.8968
Key - D	Lena*	57827	1.5049	46.36	0.9188	48.4985	0.6162	50.23
	Lena	57827	1.2579	47.13	0.66	49.936	0.3845	52.28
	Baboon*	93444	2.6619	43.88	1.8482	45.4633	2.255	44.5993
	Baboon	93444	2.0346	45.05	1.171	47.4454	1.6235	46.0262
Key - E	Lena*	57656	1.5093	46.34	0.9483	48.3613	0.6183	50.21
	Lena	57656	1.2503	47.16	0.6658	49.898	0.3605	52.56
	Baboon*	93576	2.6487	43.90	1.8139	45.5447	2.2222	44.663
	Baboon	93576	2.0229	45.07	1.1716	47.4431	1.6238	46.0255
Key - F	Lena*	55760	1.2789	47.06	0.6721	49.8567	0.3985	52.12
	Lena	55760	1.1098	47.678	0.4959	51.177	0.2396	54.33
	Baboon*	99528	2.1079	44.8923	1.232	47.2246	1.6526	45.9491
	Baboon	99528	1.6687	45.907	0.8086	49.0533	1.2409	47.1935
Key - G	Lena*	116364	1.9767	45.1715	1.4113	46.6347	1.0676	47.84
	Lena	116364	1.6374	45.989	1.0632	47.865	0.755	49.35
	Baboon*	192884	3.8383	42.2894	3.0182	43.3334	3.442	42.7627
	Baboon	192884	3.0277	43.3197	2.1618	44.7827	2.6606	43.8809
Key - H	Lena*	110891	1.7881	45.6069	1.2721	47.0855	0.9333	48.43
	Lena	110891	1.5307	46.282	0.9583	48.316	0.658	49.95
	Baboon*	193245	3.8444	42.2825	3.0907	43.2302	3.5234	42.6612
	Baboon	193245	3.0861	43.2367	2.2452	44.6183	2.6907	43.8321
Key - I	Lena*	111813	1.6711	45.9008	1.0663	47.8518	0.7775	49.22
	Lena	111813	1.4161	46.62	0.8162	49.013	0.5378	50.82
	Baboon*	199022	3.2595	42.9992	2.4182	44.2959	2.8326	43.6089
	Baboon	199022	2.5895	43.9986	1.7665	45.6596	2.2296	44.6486
Key - J	Lena*	169434	2.2429	44.6226	1.7241	45.7651	1.4246	46.59
	Lena	169434	1.8931	45.359	1.3569	46.806	1.0125	48.07
	Baboon*	292313	4.9282	41.2039	4.1728	41.9265	4.6481	41.4581
	Baboon	292313	4.0185	42.0901	3.2729	42.9814	3.7357	42.4071

Table 1 for various Key-2 using the proposed method. It's evident that from Table 1, Key-J provides high capacity and Key-A provides low capacity, moreover proposed methodology gives High PSNR over previous method (Thanikaiselvan *et al*., 2011a). By keeping Key J constant various key 1 are tabulated in Table 2.

Table 2: Key J constant by varying Key 1 for Lena and Baboon

				Channel - I Red		Channel - II Green		Channel - III Blue	
Image	Key 1(K1)	Comparison	Total No. of bits embedded	MSE	PSNR (dB)	MSE	PSNR (dB)	MSE	PSNR (dB)
Lena	k1 = 1	Method*	180454	2.8472	43.5866	2.3196	44.4766	1.852	45.4544
		Proposed	180454	2.4031	44.32	1.8255	45.51	1.3162	46.93
	k1 = 2	Method*	241201	4.9872	41.1522	4.4826	44.4766	3.8033	45.4544
		Proposed	241201	4.1899	41.90	1.7426	45.71	1.3044	46.97
	k1 = 3	Method*	310800	4.9326	41.2	4.4964	41.6022	1.3412	46.8558
		Proposed	310800	4.1631	41.93	3.473	42.72	0.9495	48.35
	k1 = 4	Method*	330012	5.943	40.3907	5.0457	41.1016	5.5904	40.6564
		Proposed	330012	4.9319	41.20	3.9877	42.12	4.1346	41.96
Baboon	k1 = 1	Method*	330012	5.943	40.3907	5.0457	41.1016	5.5904	40.6564
		Proposed	330012	5.0315	41.11	3.9708	42.14	3.9577	42.15
	k1 = 2	Method*	336404	5.2519	40.9276	4.3689	41.7271	4.7826	41.3341
		Proposed	336404	4.4711	41.62	3.4694	42.72	3.4295	42.77
	k1 = 3	Method*	358860	9.777	38.2287	8.9648	38.6054	9.3528	38.4214
		Proposed	358860	8.3023	38.93	6.8607	39.76	6.5557	39.96
	k1 = 4	Method*	375161	15.712	36.1685	15.1689	36.3213	15.6867	36.1755
		Proposed	375161	13.038	36.97	11.572	37.49	11.049	37.69

Method* -Thanikaiselvan *et al.* (2011a)

Complexity level estimation: For 8×8 pixels block case IWT, total number of blocks (N) = 1024 Number of PRNG output for randomizing the 1024 blocks:

= NpR = N!/(N-r)! = 1024p1024 = 1024!

As per DES, the complexity of each block = 2^64.

Either binary or inverted binary would be embedded hence complexity increases by 2 and 3 out 4 sub bands are used and based on key 2 either 0 or 1 then 0.5. Therefore the total complexity:

= (2^64)*(1024)! * (2) *3/4 *(.5)

These embedding are carried out in transform domain and the security level estimation reveals the firmness of the proposed stego against hackers.

CONCLUSION

It has been observed that steganography provides excellent avenue for high payload combined with imperceptibility. Literature suggests that in several techniques robustness may have been compromised, however the proposed method gives high payload (capacity) in the cover image with very little error. The algorithm is robust, as there is an option of embedding data in the transformed domain and also the option of reducing the error by determining whether direct or inverted binary maybe embedded. Key-1 and Key-2 not only provide high security but also increased capacity with the wavelet transform. The drawback of the proposed method is the computational overhead. This can be reduced by high speed computers. Thus, it can be summarized as:

- PSNR is increased in this system with intelligent use of Key-1, Key-2 and Key-3
- Because data is embedded in imperceptible areas that too in the transformed domain, the stego image can hardly raise suspicion
- Even if the stego image is transformed it would be difficult to determine what data has been embedded without Key-3 as either direct or inverted binary would be embedded. Thus capacity, imperceptibility and robustness, all the three requirements are catered to in this innovative algorithm

REFERENCES

Al-Azawi, A.F. and M.A. Fadhil, 2010. Arabic text steganography using kashida extensions with huffman code. J. Applied Sci., 10: 436-439.

Al-Frajat, A.K., H.A. Jalab, Z.M. Kasirun, A.A. Zaidan and B.B. Zaidan, 2010. Hiding data in video file: An overview. J. Applied Sci., 10: 1644-1649.

Amirtharajan, R. and R.J.B. Balaguru, 2011. Covered CDMA multi-user writing on spatially divided image. Proceedings of the Wireless ViTAE Conference, February 28-March 3, 2011, IEEE, Chennai, India, pp: 1-5.

Amirtharajan, R. and R.J.B. Balaguru, 2009. Tri-layer stego for enhanced security-a keyless random approach. Proceedings of the IEEE International Conference on Internet Multimedia Services Architecture and Applications, December 9-11, 2009, Bangalore, India, pp: 1-6.

Amirtharajan, R. and R.J.B. Balaguru, 2011. Data embedding system. WIPO Patent Application WO/2011/114196. http: // www.freepatentsonline.com /WO2011114196A1.html

Amirtharajan, R. and R.J.B. Balaguru, 2012. An intelligent chaotic embedding approach to enhance stego-image quality. Inform. Sci., (In Press).

Amirtharajan, R., D. Adharsh, V. Vignesh and R.J.B. Balaguru, 2010. PVD blend with pixel indicator-OPAP composite for high fidelity steganography. Int. J. Comput. Appl., 7: 31-37.

Amirtharajan, R., R. Subrahmanyam. P.J.S. Prabhakar, R. Kavitha and R.J.B. Balaguru, 2011. MSB over hides LSB-A dark communication with integrity. Proceedings of the IEEE 5th International Conference on Internet Multimedia Services Architecture and Applications, December 12-13, 2011, Bangalore.

Bender, W., D. Gruhl, N. Morimoto and A. Lu, 1996. Techniques for data hiding. IBM Syst. J., 35: 313-336.

Chan, C.K. and L.M. Cheng, 2004. Hiding data in images by simple LSB substitution. J. Pattern Recognit. Soc., 37: 469-474.

Cheddad, A., J. Condell, K. Curran and P. Mc Kevitt, 2010. Digital image steganography: Survey and analysis of current methods. Signal Process., 90: 727-752.

EI Safy, R.O., H.H. Zayed and A. EI Dessouki, 2009. An adaptive steganographic technique based on integer wavelet transform. Proceedings of the International Conference on Networking and Media Convergence, March 24-25, 2009, Cairo, pp: 111-117.

Hmood, A.K., B.B. Zaidan, A.A. Zaidan and H.A. Jalab, 2010a. An overview on hiding information technique in images. J. Applied Sci., 10: 2094-2100.

Hmood, A.K., H.A. Jalab, Z.M. Kasirun, B.B. Zaidan and A.A. Zaidan, 2010b. On the Capacity and security of steganography approaches: An overview. J. Applied Sci., 10: 1825-1833.

Janakiraman, S., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2012. Pixel forefinger for gray in color: A layer by layer stego. Inform. Technol. J., 11: 9-19.

Kumar, P.P. R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2011. Steg-OFDM blend for highly secure multi-user communication. Proceedings of the 2nd International Conference on Vehicular Technology, Information Theory and Aerospace and Electronic Systems Technology, February 28-March 3, 2011, IEEE, Chennai, India, pp: 1-5.

Luo, G., X. Sun and L. Xiang, 2008. Multi-blogs steganographic algorithm based on directed hamiltonian path selection. Inform. Technol. J., 7: 450-457.

Padmaa, M., Y. Venkataramani and R. Amirtharajan, 2011. Stego on 2^n:1 platform for users and embedding. Inform. Technol. J., 10: 1896-1907.

Petitcolas, F.A.P., R.J. Anderson and M.G. Kuhn, 1999. Information hiding-a survey. Proc. IEEE, 87: 1062-1078.

Provos, N. and P. Honeyman, 2003. Hide and seek: An introduction to steganography. IEEE Secur. Privacy, 1: 32-44.

Qin, J., X. Sun, X. Xiang and Z. Xia, 2009. Steganalysis based on difference statistics for LSB matching steganography. Inform. Technol. J., 8: 1281-1286.

Qin, J., X. Xiang and M.X. Wang, 2010. A review on detection of LSB matching steganography. Inf. Technol. J., 9: 1725-1738.

Rabah, K., 2004. Steganography-the art of hiding data. Inform. Technol. J., 3: 245-269.

Schneier, B., 2007. Applied Cryptography: Protocols, Algorithm and Source Code in C. 2nd Edn., Wiley, India.

Shirali-Shahreza, M. and S. Shirali-Shahreza, 2008. High capacity persian/arabic text steganography. J. Applied Sci., 8: 4173-4179.

Stefan, K. and A. Fabin, 2000. Information Hiding Techniques for Steganography and Digital Watermarking. Artech House, London, UK.

Thanikaiselvan, V., P. Arulmozhivarman, R. Amirtharajan and J.B.B. Rayappan, 2011a. Wave (let) decide choosy pixel embedding for stego. Proceedings of the International Conference on Computer, Communication and Electrical Technology, March 18-19, India, pp: 157-162.

Thanikaiselvan, V., S. Kumar, N. Neelima and R. Amirtharajan, 2011b. Data battle on the digital field between horse cavalry and interlopers. J. Theor. Applied Inform. Technol., 29: 85-91.

Thenmozhi, K., P. Praveenkumar, R. Amirtharajan, V. Prithiviraj, R. Varadarajan and R.J.B. Balaguru, 2011. OFDM+CDMA+stego = secure communication: A review. Res. J. Inform. Technol., (In Press).

Xia, Z., X. Sun, J. Qin and C. Niu, 2009. Feature selection for image steganalysis using hybrid genetic algorithm. Inform. Technol. J., 8: 811-820.

Xiang, L., X. Sun, Y. Liu and H. Yang, 2011. A secure steganographic method via multiple choice questions. Inform. Technol. J., 10: 992-1000.

Yang, B., X. Sun, L. Xiang, Z. Ruan and R. Wu, 2011. Steganography in Ms Excel Document using Text-rotation Technique Inform. Technol. J., 10: 889-893.

Yang, C.H., 2008. Inverted pattern approach to improve image quality of information hiding by LSB substitution. J. Patt. Recog. Soc., 41: 2674-2683.

Zaidan, B.B., A.A. Zaidan, A.K. Al-Frajat and H.A. Jalab, 2010. On the differences between hiding information and cryptography techniques: An overview. J. Applied Sci., 10: 1650-1655.

Zanganeh, O. and S. Ibrahim, 2011. Adaptive image steganography based on optimal embedding and robust against chi-square attack. Inform. Technol. J., 10: 1285-1294.

Zhu, J., R.D. Wang, J. Li and D.Q. Yan, 2011. A huffman coding section-based steganography for AAC audio. Inform. Technol. J., 10: 1983-1988.