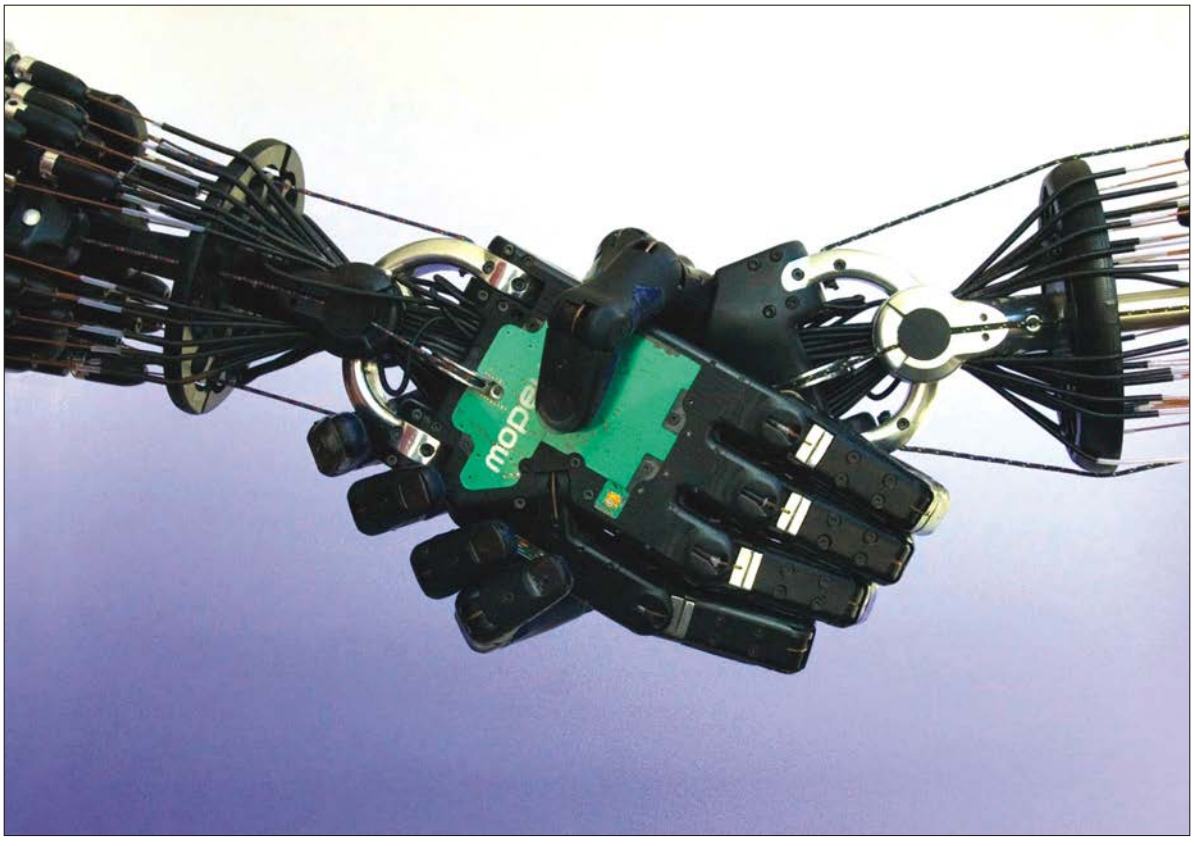

Journal of Artificial Intelligence

ISSN 1994-5450

science alert

ANSInet
an open access publisher
http://ansinet.com

Journal of Artificial Intelligence 7 (2): 54-68, 2014
ISSN 1994-5450 / DOI: 10.3923/jai.2014.54.68

PVD Based Steganography on Scrambled RGB Cover Images with Pixel Indicator

[1]V. Thanikaiselvan, [2]S. Subashanthini and [3]Rengarajan Amirtharajan
[1]School of Electronics Engineering,
[2]School of Information Technology, VIT University, Vellore, Tamilnadu, 632014, India
[3]School of Electrical and Electronics Engineering, SASTRA University, Thanjavur, 613401, India

Correspondimg Author: V. Thanikaiselvan, School of Electronics Engineering, VIT University, Vellore, Tamilnadu, 632014, India

ABSTRACT

With the rapid advancements in digital information transmission, technologies need for ensuring high level of data security, has become indispensible. In order to ensure the same, many cryptography and steganography techniques are in use. In the proposed methodology, both the techniques have been used simultaneously for incorporating a near fool proof security. Cryptography renders an image unreadable whereas, steganography aims at hiding secret information in the image. In the scrambled image, adaptive Least Significant Bit (LSB) substitution has been performed using Pixel Value Differencing (PVD) based on Pixel Indicator (PI) method for colour images. Here, secret data is embedded only in R and G planes while, B plane acts as an indicator for embedding. This methodology increases the embedding capacity by 50% compared to the existing methods in addition with a reasonable Peak Signal to Noise Ratio (PSNR) of 42 dB.

Key words: Image encryption, LSB substitution, pixel value differencing, pixel indicator method, image steganography

INTRODUCTION

With the advancements in information technology, issue of data security comes hand in hand. Large amount of data transmitted via internet needs to be made secure against malicious attacks. Secret information particularly sensitive information needs to be handled with extreme care as its misuse can create great havoc to the society. So, to make the secret information attack proof, role of various cryptographic and steganographic techniques come into picture (Cheddad *et al*., 2010; Amirtharajan and Rayappan, 2012a-d, 2013; Amirtharajan *et al*., 2013a-j; Janakiraman *et al*., 2012a, b, 2014a, b; Luo *et al*., 2011; Mohammad *et al*., 2011; Salem *et al*., 2011; Ramalingam *et al*., 2014a, b; Thien and Lin, 2003; Zhao and Luo, 2012).

Cryptography has been in practice from ancient times with its main aim being making the message unreadable by all except the authorised receiver who has the key to retain the actual message. It converts the secret information in un-intelligible form thereby, making it unreadable by a hacker. On the other hand, steganography aims at hiding data in multimedia such as image (Chan and Cheng, 2004; Amirtharajan *et al*., 2010, 2011, 2012, 2013b), audio or video files, so that secret data is invisible to the naked eye during transmission called information security (Thenmozhi *et al*., 2012; Praveenkumar *et al*., 2012a, b, 2013a, b, 2014a-j). The ideology

behind this is, if a certain feature of hidden information becomes visible, point of attack becomes evident. Various algorithms and methodologies exist for the same in hardware (Rajagopalan *et al.*, 2012a, b, 2014a-d; Janakiraman *et al.*, 2012a, b, 2014a, b).

Three main pillars of steganography are ensuring robustness (Wong *et al.*, 2007; Qi and Wong, 2005), high embedding capacity and undetectability (Wu and Tsai, 2003; Zhang and Wang, 2004; Thanikaiselvan *et al.*, 2012a-c, 2013a, b). This study proposes use of cryptography and steganography together for hiding text files in colour images which are used as cover. The RGB colour planes of the image are separated and scrambled, except the blue plane, using Arnold Cat map. Image scrambling technology is easy to realized but it is not in accordance with Kirchhoff's rules and its security is not very high. But when data is embedded in this scrambled image using steganography algorithms, a high level of security is ensured.

Blue plane of the image is used as indicator for embedding in R and G planes where the clandestine context gets pushed in the adaptive LSB values so as difference in the pixel value is not visible to the naked eye. If the pixel value of first pixel in 2×2 matrix of blue plane is even, then data is embedded in red plane else, it is embedded in green plane. Data embedding takes place by Pixel Value Differencing (PVD) method where four pixels of the 2×2 matrix of the cover used at once for embedding the data (Wu and Tsai, 2003; Zhang and Wang, 2004). Pixel indicator method (Janakiraman *et al.*, 2012a, b, 2013) is a method which can be adapted with PVD and other methods to improve the security further. In this study, PVD and pixel indicator method are used on a scrambled cover image, data is embedded adaptively in R and G plane i.e., k bits are embedded based on the level inwhich the average difference falls based on the pixel value in B plane. This technique improvises on pixel embedding capacity as well as ensuring a high level of security.

METHODOLOGY

The methods publicized here put forward a secure data hiding technique by using both cryptography and steganography techniques. The block diagram for the method is shown in Fig. 1. This technique is aimed to achieve high security by first scrambling the colour planes of cover file which is a 24 bit colour image using Arnold algorithm and then embedding the secret data in the encrypted R and G planes using a steganographic algorithm based on pixel indicator on the blue plane. For transmission, the R and G planes are descrambled and merged to form colour stego image and then transmitted thereby hiding the very essence of any data hidden. As the steganography is performed on the encrypted cover file, any attempt to search for hidden data in the transmitted file will result in garbage values. This ensures a highly secure way to transfer sensitive data as compared to use of cryptography and steganography alone.

At receiver's end, the transmitted image undergoes the encrypting process again using the key. The secret data is then extracted from the image.

Image encryption algorithm using Arnold Transform method: The colour planes are separated and Arnold Transform is used as the encryption technique for scrambling pixels in these R and G planes. Arnold Transform is applied to the planes in the spatial domain itself. For encryption of the cover image, Eq. 1 is used:

$$\begin{bmatrix} a' \\ b' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} \bmod M,\ a, b \in \{0,1,2...N-1\} \quad (1)$$

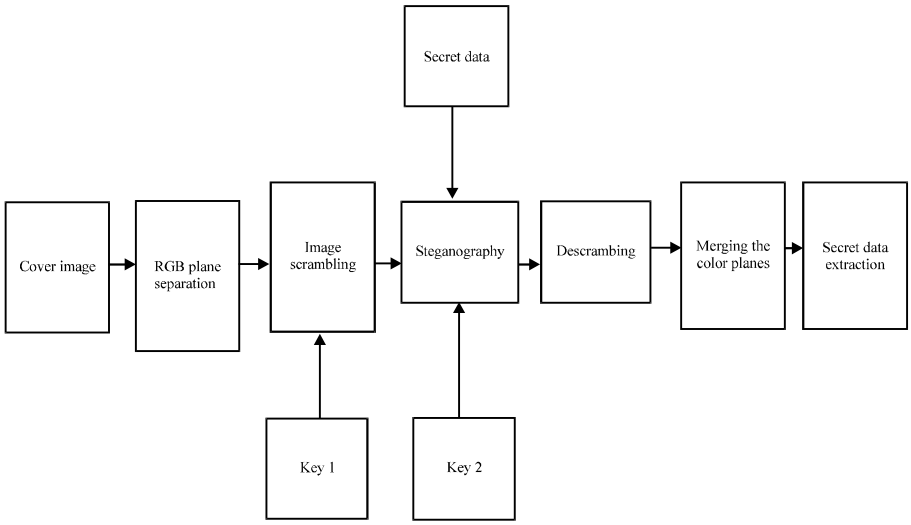

Fig. 1: Proposed block diagram

where:

$$AT = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$$

is the transfromation matrix and M×M pixels is the size of the cover image. Here, the dimension of the cover image is 512×512 pixels. Also, a, b are the pixel location of the original image, a', b' as a pixel location of the scrambled image. The location of one pixel is changed multiple times. The number of times it is changed is the key 1 for the encryption process and is stored as the number of iterations. The process is same for both the planes.

The Arnold Transform method of encryption is periodic in nature. It is robust, quick and has high confidentiality. After Arnold transformation of the image, the pixel's location is transformed but this transformation will not change the values of the pixel values hence, the image histogram is the same.

Image steganography: Now, the R and G planes have been encrypted, the secret data is embedded in an order in the R and G plane depending on whether the left topmost corner pixel in the 2×2 matrix of blue plane is even or odd. The secret data can be a text file which has been converted into binary. In this study, only binary data has been embedded in R and G planes according to Table 1.

- **LSB substitution method:** It is the technique wherein the secret data is embedded into encrypted pixel by changing the LSB of the pixel so that it holds covert bits. Let, C is the original 8-bit R or G plane of 512×512 pixels represented as shown in Eq. 2:

$$Ck = \{a_{ij} | 0 \le i, j \le 511, a_{ij} \in \{0,1, \ldots., 256\}\} \quad (2)$$

Secret (n-bit) is denoted by M as shown in Eq. 3:

Table 1: Pixel indicator method

Indicator-Blue plane	Channel 1	Channel 2
Even	First embed n bits in Red plane	Embed next n bits in Green plane
Odd	First embed n bits in Green plane	Embed next n bits in Red plane

$$Mg = \{n_i | 0 \le i < m, n_i \in \{0, 1\}\} \quad (3)$$

where, m-bit secret message has to be embedded into the k (k may be 1, 2, 3, 4) rightmost LSBs of the colour planes R and G. This m-bit binary message is converted to its decimal value by combining k bits together (Z_{ip}). The substitution is done by using the Eq. 4:

$$a_{ij}' = a_{ij} - \text{mod}(a_{ij}, 2^k) + Z_{ip} \quad (4)$$

The new pixel value, a_{ij}', has the secret data embedded in last k bits. As data gets infixed only in LSBs, the pixel value does not change significantly and is not visible to the human eye.

- **Pixel value differencing:** The encrypted cover file is taken and is divided into sub-blocks of 2×2 pixels. An adaptive method is used to embed the data, i.e., the total bits rooted in each location is not the same. It is in accordance with a condition. This makes the data embedding procedure even more robust.

  A threshold value Th is taken for the embedding process. The range of Th is $2^{kl} \le Th \le 2^{kh}$, where kl and kh are the number of bits embedded in the lower threshold and upper threshold, respectively.

  A sub-block of 2×2 pixels is taken from the image. Out of the 4 pixels, the minimum (P_{min}) is found. Then using formula in Eq. 5, value of delta is estimated. According to the relation of Delta with Th, either higher level embedding (if Delta>Th) or lower level embedding (if Delta<Th) is performed, i.e., either kh or kl bits of data is embedded, respectively.

$$\text{Delta} = \frac{\sum_{i=1}^{4}(p_i - p_{min})}{3} \quad (5)$$

where, P_1, P_2, P_3, P_4 are the four pixel values of the 2×2 sub-block.

This method for steganography gives higher embedding capacity and better image quality. The secret data is secure as the key 2 (i.e., the threshold value Th, kl and kh) needs to be known for the extraction of information. Without the key, there is no way of extracting the data.

Decryption: Before the transmission of the stego image, the R and G planes are decrypted so as to get the original cover image. This is done so that the hackers do not suspect the presence of any information in the image. If the hackers try to get information then, it will result in garbage values as the decryption process has changed the sequence inwhich data was stored. Equation 6 is used for the decryption process; it is the inverse of the Arnold Transform Matrix:

$$\begin{bmatrix} a' \\ b' \end{bmatrix} = \begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} \text{ mod } M, a, b \in \{0, 1, 2..M-1\} \quad (6)$$

where:

$$AT = \begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix}$$

is the inverse transformation matrix and M×M is the cover's dimension which is 512×512. Also, a, b are the pixel location of the scrambled image, a', b' as a pixel location of the descrambled image. The multiplication i.e., pixel location change is performed as many times as when it was scrambled. The decrypted image is now ready for transmission and the colour planes are merged after descrambling.

Stego extraction: The first step of the stego extraction process is to scramble the individual R and G planes again using Arnold Transform and the key 1 as described above. The key 2 contains the information about the Threshold Th and the kl and kh, i.e., bits inserted at different levels. A sub-block of 2×2 pixels is taken from the R, G and B planes. Out of the 4 pixels, find the minimum pixel value for the R and G planes and find the delta value using Eq. 5, separately for the R and G planes. If the remainder after dividing the left topmost pixel in sub-block in B plane be 0, then bits are primarily extracted from the R plane followed by the G plane. On the other hand, if the remainder is 1, bits are first extracted from the G plane and then from R plane. According to the relation of the individual delta of the R and G planes with THz, either kh bits of information (if Delta>Th) or kl bits (if Delta<Th) is extracted. Thus, the information embedded has been successfully extracted.

EMBEDDING ALGORITHM

Step 1: Read a 512×512 RGB image as the Cover Image

Step 2: Separate the image into the R, G, B planes. The embedding process is done only on the Red and Green planes. And the Blue plane decides the order in which the binary message is embedded in these planes

Step 3: Apply image scrambling Algorithm using Arnold Transform Method on the Red and Green planes

- **Step 3.1:** Calculate the size of the image and store it in N, i.e., N=512
- **Step 3.2:** Run two loops for the rows and columns. Find the new location of the pixel using the Eq. 1
- **Step 3.3:** The pixel value of the original pixel location is assigned to the new pixel location
- **Step 3.4:** Steps 2 and 3 are repeated for number of times one wants to change the location of each pixel. This number of iterations serves as the key for the encryption process
- **Step 3.5:** Supply the scramble image for the next step for steganography

Step 4: Apply Pixel Value Indicator based steganography to the image

- **Step 4.1:** The R, G and B planes are divided into sub-blocks of 2×2 pixels. The sub-block is extended from the top left corner rightwards
- **Step 4.2:** The top left corner pixel of the 2×2 pixels of the B plane decides the order in which the message is embedded in the plane. The remainder is calculated after dividing the top left corner pixel of the 2×2 pixels of the B plane by 2. If the remainder is 0 then first embed in the plane R and next G. Else if the remainder is 1 first embed in the G followed by R
- **Step 4.3:** A threshold value Th is taken for the embedding process. The range of Th is $2^{kl} \leq Th \leq 2^{kl}$, where kl and kh are the number of bits embedded in the lower threshold and upper threshold, respectively
- **Step 4.4:** Let the 4 pixel values in the sub block be R_1, R_2, R_3 and R_4 of the R plane and G_1, G_2, G_3 and G_4. The minimum of these 4 pixels is found and stored in R_{min} and G_{min}

Step 4.5: Now find Delta for the 4 pixels for both the planes using the Eq. 5. The Delta is symbolized as D1 and D2 respectively for the R and G planes

Step 4.6: Now, if the remainder is 0, embed the data first in planes R and G. D1 value determines the bits for embedding for R plane and D2 value for the G plane

Step 4.7: If the remainder is 1then first veil data in plane G after that R. D2 value determines the bits for embedding for G plane; D1 value for the R plane

Step 4.8: If D1>Th or D2>Th then kh bits of information get rooted in each sub-block pixel through LSB substitution method in the R and G planes, respectively

Step 4.9: If D1<=Th or D2<=Th, then kl number of bits of information gets rooted in each sub-block pixel by LSB substitution method in R and G planes, respectively

Step 4.10: Steps 4.1 to 4.9 are repeated till all the pixels have undergone this process

Step 4.11: Generate a Steganography image

Step 5: Apply Descrambling algorithm with Arnold Transform to the R and G planes:

Step 5.1: Calculate the size of the image and store it in N, i.e., N = 512

Step 5.2: Run two loops for the rows and columns. Find the new location of the pixel using Eq. 6

Step 5.3: The pixel value of the original pixel location is assigned to the new pixel location

Step 5.4: Steps 2 and 3 are repeated the same number of times as the value stored in the key1

Step 5.5: The differed three planes are combined to get one colour image. The image is now ready for transmission

EXTRACTION ALGORITHM

The first step of the stego extraction process is to separate the R, G and B planes of the colour image received and then scramble the R and G planes again using Arnold Transform and the key as described above. Now the image is of the form in which the data was embedded:

Step 1: The R, G and B plane is divided into sub-blocks of 2×2 pixels. The sub-block is extended from the top left corner rightwards

Step 2: The top left corner pixel of the 2×2 pixels of the B plane decides the order in which the message is extracted from the plane. Find the remainder after dividing the top left corner pixel of the 2×2 pixels of the B plane by 2. If the remainder is 0 then first extract from the R and G planes. Else if the remainder is 1, first extract the G and R plane bits

Step 3: Let 4 pixel values in the sub block be R_1, R_2, R_3 and R_4 of the R plane and G_1, G_2, G_3 and G_4. The minimum of these 4 pixels is found and stored in R_{min} and G_{min}

Step 4: Now find Delta for the 4 pixels for both the planes using the Eq. 5. The delta is symbolized as D1 and D2 respectively for the R and G planes

Step 5: Now, if the remainder is 0, extract the data first from the R plane and then from the G plane. The number of bits to be extracted is decided by the D1 value for R plane and D2 value for the G plane

Step 6: If the remainder is 1 then first extract the data from the G plane and then from the R plane. D2 value fixes the embedding bits for G plane whereas the D1 value for the R plane

- If D1>Th or D2>Th, then kh bits of information are extracted from each pixel using $mod(R_i,2^{kh})$ or $mod(G_i,2^{kh})$
- If D1<=Th or D2<=Th, then extract kl bits of information from each pixel using $mod(R_i,2^{kl})$ or $mod(G_i,2^{kl})$

Step 7: The extracted information is concatenated together to form one string of binary data

Step 8: Steps 1 to 7 are repeated till all the pixels have undergone this process

Thus, the binary information that was embedded has been successfully extracted. Now, convert the binary information to the string format.

RESULTS AND DISCUSSION

Experiments using Matlab software have been performed on 5 colour images with size 512×512. PSNR values for each red and Green plane along with number of bits embedded in each scrambled

image has been calculated. A text file has been used as surreptitious content that gets rehabilitated from its ASCII value to binary to make it suitable for embedding in the scrambled cover image. The PSNR is used for estimating scrambled stego image's quality. For a P×Q gray scale image, PSNR is calculated as shown in Eq. 7:

$$PSNR = 10\times \log_{10}\left[\frac{255\times 255\times P\times Q}{\sum_{i=1}^{P}\sum_{j=1}^{Q}\left(a_{i,j}-b_{i,j}\right)}\right](dB) \quad (7)$$

where, $a_{i,j}$ pixels in ith row and jth column of cover whereas, $b_{i,j}$ is the same as that of stego.

Stego images generated for this proficiency are shown from Fig. 2-7. Figure 2 shows five colour images of size 512×512 which are the original images. Figure 3 and 4 shows the result after scrambling the R and G plane using Arnold Algorithm. The scrambling can be performed n number of times. Figure 5 and 6 shows stego R and G images with data embedded inside using PVD and LSB substitution. Figure 7 shows descrambled stego colour images obtained after merging the RGB planes transmitted through a suitable channel. As can be seen, no significant difference can be noticed in original images and descrambled stego images.

Table 2 contains the capacity and the PSNR for five different images for varied threshold and levels of embedding.

Fig. 2(a-e): Cover images of size 512×512, (a) Peppers, (b) Baboon, (c) Castle, (d) Barbara and (e) Boat

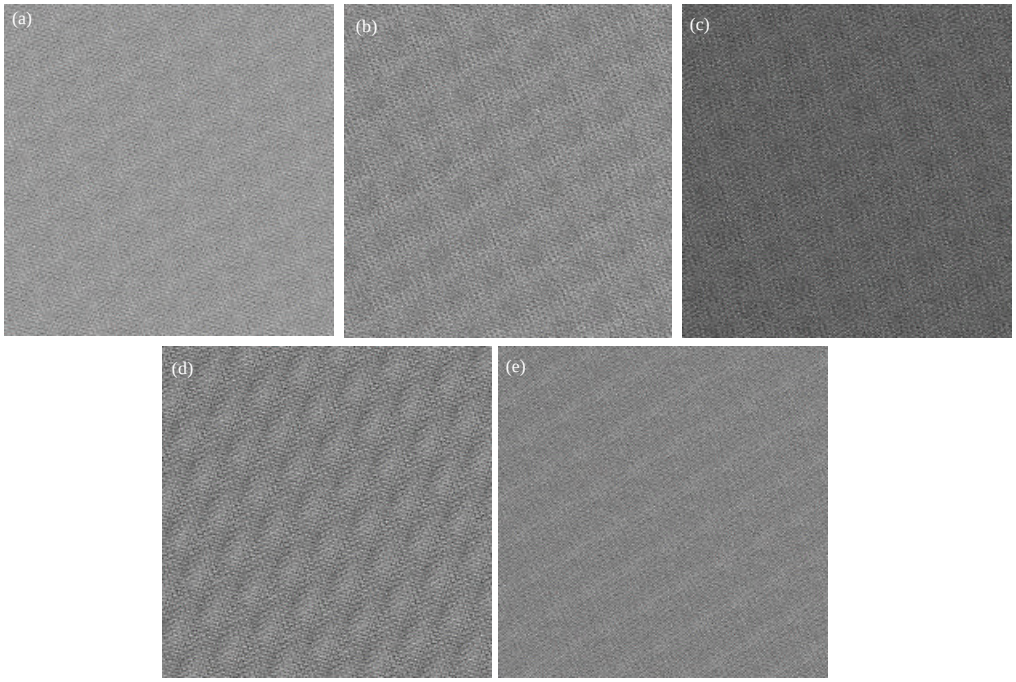

Fig. 3(a-e): R plane scrambled images with size 512×512, (a) Peppers, (b) Baboon, (c) Castle, (d) Barbara and (e) Boat

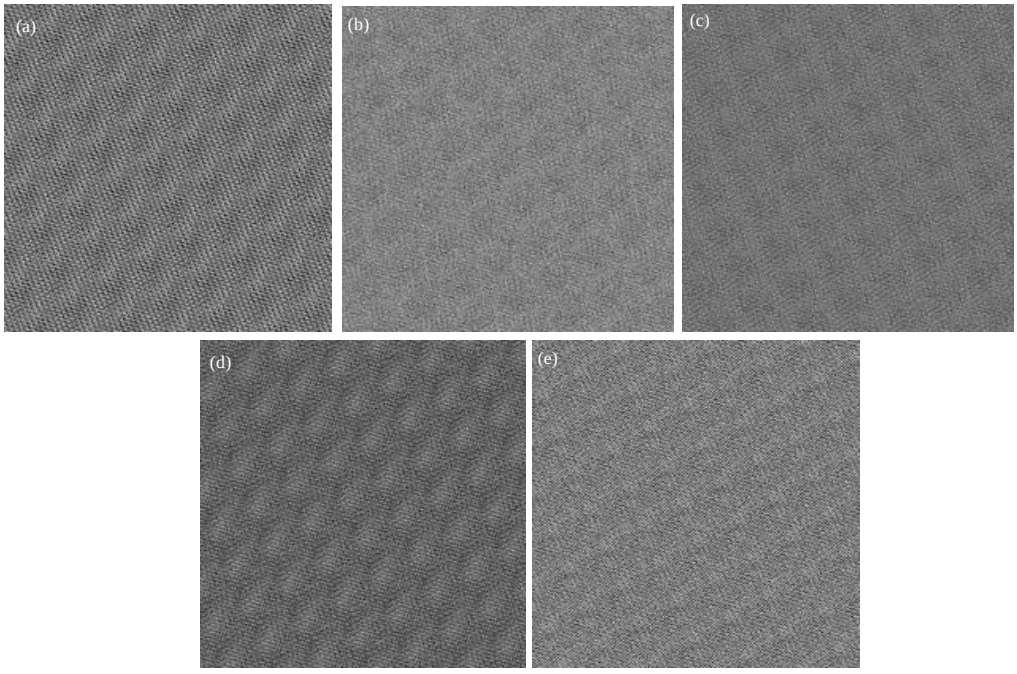

Fig. 4(a-e): G plane scrambled images of size 512×512, (a) Peppers, (b) Baboon, (c) Castle, (d) Barbara and (e) Boat

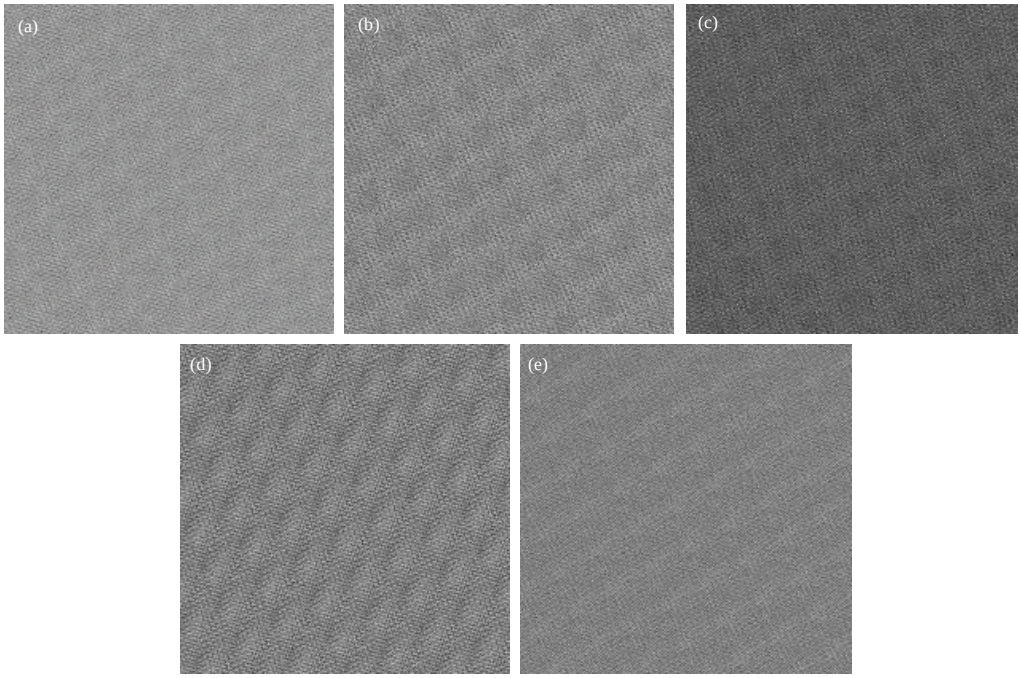

Fig. 5(a-e): Stego.R plane scrambled images of size 512×512, (a) Peppers, (b) Baboon, (c) Castle, (d) Barbara and (e) Boat

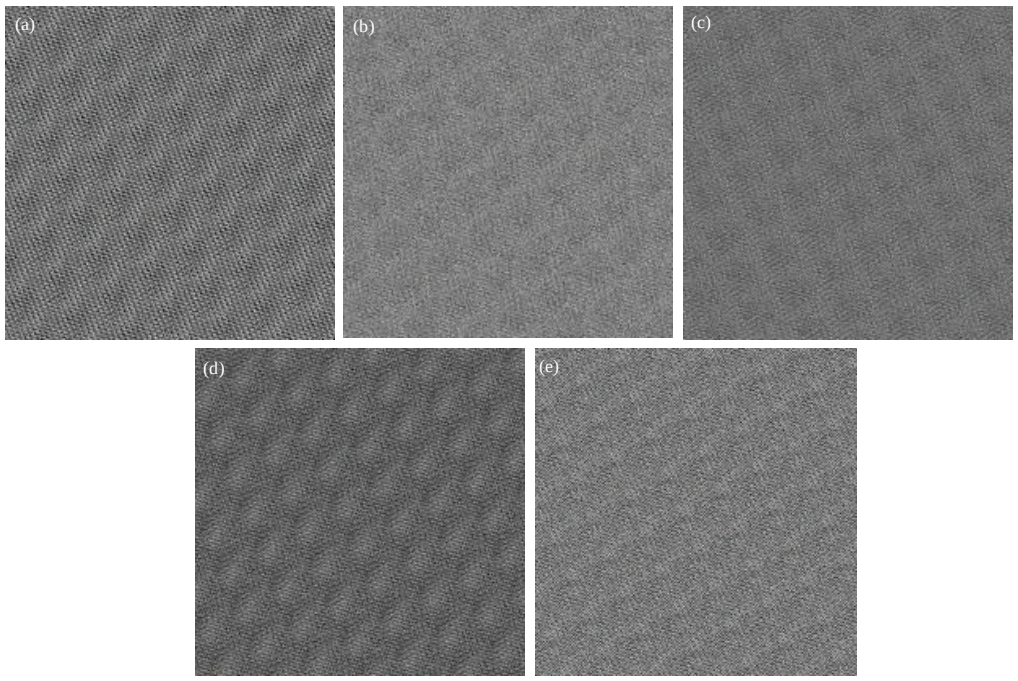

Fig. 6(a-e): Stego. G plane scrambled images with size 512×512, (a) Peppers, (b) Baboon, (c) Castle, (d) Barbara and (e) Boat

Fig. 7(a-e): Descrambled Stego colour images with size 512×512, (a) Peppers, (b) Baboon, (c) Castle, (d) Barbara and (e) Boat

In Table 2, various threshold values as Th = 5, 6, 12, 18 with various kl-kh values have been taken and PSNR value for Red and Green planes along with bit embedding capacity has been calculated. For example, at Th = 5, if Delta<=Th, 2 bits are embedded and at Delta>Th, 3 bits are embedded in a 4 pixel block. It can be observed that with the increase in threshold value, PSNR reduces but the embedding capacity (in bits) increases at the same time.

The comparative analysis for the difference in the levels of embedding when the scrambled R and G planes are used for embedding versus when original R and G planes are used is shown in Table 3. As can be seen, the capacity increases with the scrambling of R and G planes as compared to using original R and G planes.

Table 4 shows the comparative analysis between proposed and other spatial domain steganography methods. Scrambled cover image is well suitable for PVD based steganography because it offers high capacity and high PSNR over other methods. For the comparative analysis, a 256×256 RGB baboon image is taken as a cover image. In RGB images one pixel value takes 24 bits for showing all color combinations. In the proposed method, total 393158 bits are embedded in a single image with PSNR of 42.5 dB (average). This shows that the proposed method has high capacity with high imperceptibility than the other methods. Moreover, Red and Green planes are only used for embedding process and the Blue plane is used as an indicator for embedding process.

Table 2: Capacity and PSNR values for various T, kl and kh

	T = 5, 2-3 (kl-kh)			T = 6, 2-3 (kl-kh)		
Image	Capacity	PSNR_R (dB)	PSNR_G (dB)	Capacity	PSNR_R (dB)	PSNR_G (dB)
Peppers	1572520	42.77	42.81	1572300	42.76	42.81
Baboon	1572632	42.74	42.75	1572428	42.74	42.75
Castle	1572464	42.73	42.79	1572248	42.73	42.79
Barbara	1572656	42.75	42.80	1572576	42.76	42.78
Boat	1572460	42.79	42.69	1572236	42.79	42.70
	T = 12 3-4(kl-kh)			T = 18 3-5(kl-kh)		
Image	Capacity	PSNR_R (dB)	PSNR_G (dB)	Capacity	PSNR_R (dB)	PSNR_G (dB)
Peppers	2087704	36.15	36.34	2593352	30.49	30.57
Baboon	2091272	36.15	36.12	2602920	30.30	30.39
Castle	2088520	36.13	36.23	2594792	30.38	30.42
Barbara	2092800	36.11	36.16	2607776	30.28	30.21
Boat	2092800	36.11	36.16	2607776	30.28	30.21

Table 3: Comparative analysis between with and without scrambling cover image

	With scrambling R and G			Without scrambling R and G		
Image	Capacity	PSNR_R (dB)	PSNR_G (dB)	Capacity	PSNR_R (dB)	PSNR_G (dB)
Peppers	1572520	42.77	42.81	1179216	46.68	46.58
Baboon	1572632	42.74	42.75	1507836	43.24	43.12
Castle	1572464	42.73	42.79	1238936	45.69	45.79
Barbara	1572656	42.75	42.80	1286404	45.12	45.24
Boat	572460	42.79	42.69	1435976	43.80	43.69

Table 4: Comparative analysis for determination of cover image of baboon between other spatial domain methods

	Red		Green		Blue			
PI methods	MSE	PSNR (dB)	MSE	PSNR (dB)	MSE	PSNR (dB)	Bits per pixel	No. of bits Embedded
Proposed methods	3.7420	42.40	3.6560	42.5000	Indicator plane		5.9990	393158
Amirtharajan *et al*. (2013b)	0.4754	51.35	0.2587	54.0024	4.6733	41.4345	1.9858	130144
Amirtharajan *et al*. (2012)	2.3702	44.39	2.3255	44.4657	2.3619	44.3981	3.9232	257108
Amirtharajan *et al*. (2011)	1.5540	46.21	1.5544	46.2151	1.5904	46.1157	2.3975	157121
Amirtharajan *et al*. (2010)	2.6100	43.96	2.6500	43.8800	2.72	43.7700	2.5100	164496

CONCLUSION

This study recommends a steganographic data security algorithm for ensuring high level of data security. First, the Cover Image has been scrambled using Arnold algorithm and data has been embedded in the scrambled image to incorporate high degree of randomness using PVD and k-bit LSB substitution according to pixel indicator which is blue plane in this case. It has been observed that as the threshold value goes up, the embedding capacity increases significantly but there is a decrease in PSNR value that is the picture quality degrades. It is vivid that the embedding competence increases through the use of scrambling R and G planes as compared to using original R and G planes, in addition to increasing security. This scheme majors in the grounds

of entrenching capability and making secret data fool proof. However, there is a tradeoff between PSNR and embedding capacity at high threshold values. Improving the same will be our future endeavor.

REFERENCES

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. Applic., 7: 31-37.

Amirtharajan, R., R.R. Subrahmanyam, P.J.S. Prabhakar, R. Kavitha and J.B.B. Rayappan, 2011. MSB over hides LSB: A dark communication with integrity. Proceedings of the IEEE 5th International Conference on Internet Multimedia Systems Architecture and Application, December 12-14, 2011, Bangalore, Karnataka, India, pp: 1-6.

Amirtharajan, R. and J.B.B. Rayappan, 2012a. An intelligent chaotic embedding approach to enhance stego-image quality. Inform. Sci., 193: 115-124.

Amirtharajan, R. and J.B.B. Rayappan, 2012b. Brownian motion of binary and gray-binary and gray bits in image for stego. J. Applied Sci., 12: 428-439.

Amirtharajan, R. and J.B.B. Rayappan, 2012c. Inverted pattern in inverted time domain for icon steganography. Inform. Technol. J., 11: 587-595.

Amirtharajan, R. and J.B.B. Rayappan, 2012d. Pixel authorized by pixel to trace with SFC on image to sabotage data mugger: A comparative study on PI stego. Res. J. Inform. Technol., 4: 124-139.

Amirtharajan, R., J. Qin and J.B.B. Rayappan, 2012. Random image steganography and steganalysis: Present status and future directions. Inform. Technol. J., 11: 566-576.

Amirtharajan, R. and J.B.B. Rayappan, 2013. Steganography-time to time: A review. Res. J. Inform. Technol., 5: 53-66.

Amirtharajan, R., G. Devipriya, V. Thanikaiselvan and J.B.B. Rayappan, 2013a. High capacity triple plane embedding: A colour stego. Res. J. Inform. Technol., 5: 373-382.

Amirtharajan, R., K. Karthikeyan, M. Malleswaran and J.B.B. Rayappan, 2013b. Kubera kolam: A way for random image steganography. Res. J. Inform. Technol., 5: 304-316.

Amirtharajan, R., K.M. Ashfaaq, A.K. Infant and J.B.B. Rayappan, 2013c. High performance pixel indicator for colour image steganography. Res. J. Inform. Technol., 5: 277-290.

Amirtharajan, R., M.V. Abhiram, G. Revathi, J.B. Reddy, V. Thanikaiselvan and J.B.B. Rayappan, 2013d. Rubik's cube: A way for random image steganography. Res. J. Inform. Technol., 5: 329-340.

Amirtharajan, R., P. Archana and J.B.B. Rayappan, 2013e. Why image encryption for better steganography. Res. J. Inform. Technol., 5: 341-351.

Amirtharajan, R., P.S. Priya and J.B.B. Rayappan, 2013f. Pixel indicated user indicator: A muxed stego. Res. J. Inform. Technol., 5: 73-86.

Amirtharajan, R., R. Subrahmanyam, J.N. Teja, K.M. Reddy and J.B.B. Rayappan, 2013g. Pixel indicated triple layer: A way for random image steganography. Res. J. Inform. Technol., 5: 87-99.

Amirtharajan, R., S. Sulthana and J.B.B. Rayappan, 2013h. Seeing and believing is a threat: A visual cryptography schemes. Res. J. Inform. Technol., 5: 435-441.

Amirtharajan, R., S.D. Roy, N. Nesakumar, M. Chandrasekar, R. Sridevi and J.B.B. Rayappan, 2013i. Mind game for cover steganography: A refuge. Res. J. Inform. Technol., 5: 137-148.

Amirtharajan, R., V. Rajesh, P. Archana and J.B.B. Rayappan, 2013j. Pixel indicates, standard deviates: A way for random image steganography. Res. J. Inform. Technol., 5: 383-392.

Chan, C.K. and L.M. Cheng, 2004. Hiding data in images by simple LSB substitution. Pattern Recognit., 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.

Janakiraman, S., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2012a. Firmware for data security: A review. Res. J. Inform. Technol., 4: 61-72.

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

Janakiraman, S., S. Rajagopalan, K. Thenmozhi, H.N. Upadhyay and J. Ramanathan *et al*., 2013. Captivating CODEC Stego (CCS): A cover on camouflage. Res. J. Inform. Technol., 5: 160-170.

Janakiraman, S., J. Chakravarthy, B. Radhakrishnan, K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2014a. Cover as key and key as data: An inborn stego. Inform. Technol. J., 13: 1969-1976.

Janakiraman, S., K.V.S.K. Kumar, R.R.K. Reddy, A. Srinivasulu, R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2014b. Humming bird with coloured wings: A feedback security approach. Inform. Technol. J., 13: 2022-2026.

Luo, H., Z. Zhao and Z.M. Lu, 2011. Joint secret sharing and data hiding for block truncation coding compressed image transmission. Inform. Technol. J., 10: 681-685.

Mohammad, N., X. Sun and H. Yang, 2011. An excellent Image data hiding algorithm based on BTC. Inform. Technol. J., 10: 1415-1420.

Praveenkumar, P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2012a. Phase for face saving-a multicarrier stego. Procedia Eng., 30: 790-797.

Praveenkumar, P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2012b. Regulated OFDM-role of ECC and ANN: A review. J. Applied Sci., 12: 301-314.

Praveenkumar, P., M. Nagadinesh, P. Lakshmi, K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2013a. Convolution and viterbi EN(DE)coders on OFDM hides, rides and conveys message-A neural STEGO. Proceedings of the International Conference on Computer Communication and Informatics, January 4-6, 2013, Coimbatore, pp: 1-5.

Praveenkumar, P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2013b. Can we reduce PAPR? OFDM+PTS+SLM+STEGO: A novel approach. Asian J. Sci. Res., 6: 38-52.

Praveenkumar, P., G.S. Hemalatha, B. Reddy, K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2014a. Secret link through simulink: A stego on OFDM channel. Inform. Technol. J., 13: 1999-2004.

Praveenkumar, P., K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2014b. Data puncturing in OFDM channel: A multicarrier stego. Inform. Technol. J., 13: 2037-2041.

Praveenkumar, P., K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2014c. Inserted embedding in OFDM channel: A multicarrier stego. Inform. Technol. J., 13: 2017-2021.

Praveenkumar, P., K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2014d. Purposeful error on OFDM: A secret channel. Inform. Technol. J., 13: 1985-1991.

Praveenkumar, P., K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2014e. Reversible steganography on OFDM channel-a role of RS coding. Inform. Technol. J., 13: 2052-2056.

Praveenkumar, P., K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2014f. Spread and hide-a stego transceiver. Inform. Technol. J., 13: 2061-2064.

Praveenkumar, P., K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2014g. Stego in multicarrier: A phase hidden communication. Inform. Technol. J., 13: 2011-2016.

Praveenkumar, P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2014h. Double layer encoded encrypted data on multicarrier channel. J. Applied Sci., 14: 1689-1700.

Praveenkumar, P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2014i. Sub carriers carry secret: An absolute stego approach. J. Applied Sci., 14: 1728-1735.

Praveenkumar, P., R. Deepak, K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2014j. Reversible steganography on OFDM channel: A role of cyclic codes. Inform. Technol. J., 13: 2047-2051.

Qi, X. and K. Wong, 2005. An adaptive DCT-based mod-4 steganographic method. Proceedings of the IEEE International Conference on Image Processing, Volume 2, September 11-14, 2005, Genoa, Italy, pp: II-297-II-300.

Rajagopalan, S., R. Amirtharajan, H.N. Upadhyay and J.B.B. Rayappan, 2012a. Survey and analysis of hardware cryptographic and steganographic systems on FPGA. J. Applied Sci., 12: 201-210.

Rajagopalan, S., S. Janakiraman, H.N. Upadhyay and K. Thenmozhi, 2012b. Hide and seek in silicon: Performance analysis of Quad block Equisum Hardware Steganographic systems. Procedia Eng., 30: 806-813.

Rajagopalan, S., H.N. Upadhyay, S. Varadarajan, J.B.B. Rayappan and R. Amirtharajan, 2014a. Gyratory assisted info hide-a nibble differencing for message embedding. Inform. Technol. J., 13: 2005-2010.

Rajagopalan, S., K. Pravallika, R. Radha, H.N. Upadhyay, J.B.B. Rayappan and R. Amirtharajan, 2014b. Stego on song-an amalgam of VI and FPGA for hardware info hide. Inform. Technol. J., 13: 1992-1998.

Rajagopalan, S., P.J.S. Prabhakar, M.S. Kumar, N.V.M. Nikhil, H.N. Upadhyay, J.B.B. Rayappan and R. Amirtharajan, 2014c. MSB based embedding with integrity: An adaptive RGB Stego on FPGA platform. Inform. Technol. J., 13: 1945-1952.

Rajagopalan, S., Y. Ravishankar, H.N. Upadhyay, J.B.B. Rayappan and R. Amirtharajan, 2014d. Modeling combo PR Generator for Stego Storage Self Test (SSST). Inform. Technol. J., 13: 1936-1944.

Ramalingam, B., R. Amirtharajan and J.B.B. Rayappan, 2014a. LCC-LSB-FPGA stego-A reconfigurable security. J. Applied Sci., 14: 2139-2148.

Ramalingam, B., R. Amirtharajan and J.B.B. Rayappan, 2014b. Stego on FPGA: An IWT approach. Sci. World J. 10.1155/2014/192512

Salem, Y., M. Abomhara, O.O. Khalifa, A.A. Zaidan and B.B. Zaidan, 2011. A review on multimedia communications cryptography. Res. J. Inform. Technol., 3: 146-152.

Thanikaiselvan, V., P. Arulmozhivarman, J.B.B. Rayappan and R. Amirtharajan, 2012a. Graceful graph for graceful security-towards a STE (G) Raph. Res. J. Inform. Technol., 4: 220-227.

Thanikaiselvan, V., P. Arulmozhivarman, R. Amirtharajan and J.B.B. Rayappan, 2012b. Horse riding and hiding in image for data guarding. Procedia Eng., 30: 36-44.

Thanikaiselvan, V., P. Arulmozhivarman, R. Amirtharajan and J.B.B. Rayappan, 2012c. Wavelet Pave the Trio travel for a secret mission: A stego vision. Global Trends Inf. Syst. Software Appl., 270: 212-221.

Thanikaiselvan, V., K. Santosh, D. Manikanta and R. Amirtharajan, 2013a. A new steganography algorithm against chi square attack. Res. J. Inform. Technol., 5: 363-372.

Thanikaiselvan, V., P. Arulmozhivarman, S. Subashanthini and R. Amirtharajan, 2013b. A graph theory practice on transformed image: A random image steganography. Sci. World J. 10.1155/2013/464107

Thenmozhi, K., P. Praveenkumar, R. Amirtharajan, V. Prithiviraj, R. Varadarajan and J.B.B. Rayappan, 2012. OFDM+CDMA+Stego = Secure communication: A review. Res. J. Inform. Technol., 4: 31-46.

Thien, C.C. and J.C. Lin, 2003. A simple and high-hiding capacity method for hiding digit-by-digit data in images based on modulus function. Pattern Recognit., 36: 2875-2881.

Wong, K., X. Qi and K. Tanaka, 2007. A DCT-based Mod4 steganographic method. Signal Process., 87: 1251-1263.

Wu, D.C. and W.H. Tsai, 2003. A steganographic method for images by pixel-value differencing. Pattern Recogn. Lett., 24: 1613-1626.

Zhang, X. and S. Wang, 2004. Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security. Pattern Recognit. Lett., 25: 331-339.

Zhao, Z. and H. Luo, 2012. Reversible data hiding based on Hilbert curve scan and histogram modification. Inform. Technol. J., 11: 209-216.