Research Journal of Information Technology

ISSN 1815-7432

Academic Journals Inc.

www.academicjournals.com

Research Journal of Information Technology 5 (2): 181-190, 2013
ISSN 1815-7432 / DOI: 10.3923/rjit.2013.181.190

Graceful Labeling of Assignable Information Hiding in Image

[1]G. Sathiamoorthy, [2]T.N. Janakiraman, [3]N. Sairam, [4]N.R. Raajan, [4]K.S. Mathavan, [4]P. Praveenkumar, [4]R. Krishnakumar, [4]M. Malligaraj and [4]K. Karthikeyan
[1]School of Humanities and Sciences, SASTRA University Thanjavur, Tamil Nadu, India
[2]NIT, Trichy, SASTRA University Thanjavur, Tamil Nadu, India
[3]School of Computing, SASTRA University Thanjavur, Tamil Nadu, India
[4]School of Electrical and Electronics Engineering, SASTRA University Thanjavur, Tamil Nadu, India

Corresponding Author: G. Sathiamoorthy, School of Humanities and Sciences, SASTRA University Thanjavur, Tamil Nadu, India

ABSTRACT

Ever since the world war, the call for information security raised. The explosion in World Trade Centre alarmed the people to work more towards secured travel of data. Then Steganography came to rescue, as here communication is also obscured. In many of the applications size of the secret data will be less than that of the size of the Cover Image which results in wastage of bandwidth. In this proposed study, multi-user embedding is carried out and is implemented for 5 users. Secret data of all the users is first encrypted by using Advanced Encryption Standarad (AES) and then by Ron Rivest, Adi shamir and Leonard Adleman(RSA) which escalates the complexity. A graceful graph is used for fixing the randomized order of embedding. Priority in the order of embedding among the five users will be changed during every cycle.

Key words: Information hiding, LSB substitution, RSA, graceful labeling

INTRODUCTION

The hackers also grew up to counter these safety measures. Rupert Murdoch, Julian Assange to name a few. Hence, Emphasis given on a powerful algorithm. Conventional steganography involves the concept of one image per user, where only one user can embed the information within an image. The proposed work here has gone up a level where up to five users can use a single colour image to embed and transmit their data. Each user has been assigned a pixel to embed ones data and after embedding, one has to go to other pixel for embedding which will be determined by the Graceful Labeling methodology and the order of user index will be all combinations of five users i.e., 1, 2, 3, 4, 5; 3, 1, 4, 2, 5 and so on. This introduces the randomization in the order of embedding. Randomization in the selection of planes is done by using a slightly altered PIT. The strength of the whole system is enhanced further by the RSA public crypto system and AES. Each user first has to encrypt his data by using AES and then RSA will be employed. This Randomized multi-user steganography amplify the strength of the system and thus making attack nohow. Finally the quality of the proposed system is justified using the parameters MSE and PSNR.

A decade back, Information technology was just a branch of study. But now it's become the way of life with so many developments and new technology added in it. In the world of internet, people have reached such great heights that anything is just but surely possible. The communication sector taking IT and its developments as a platform has also made renovations in itself. The Stone Age communication was replaced by paper and then to the mobiles, then was the computer laptops and presently we are in the TAB's era.

This all innovations exhibit major platform is the Internet and again the base being the Information technology. With so many advantages of IT, there are again equivalent or rather more number of disadvantages and one of the major being security. The security of data in this mode of communication is almost nothing. A deeper insight into it, leads to a conclusion that the inventor of the technology is itself the creator the security issues.

So to tackle such crisis of security, lot of new methods and algorithms of encryption for the data have been formulated and were collectively called "Cryptography". The then efficient means of security for the data was widely accepted. But over time, as this method leaves out traces of data modification, the search started again.

Then into the race was steganography, with much vibrant and safer algorithms to just tackle any security in any domain. May it be audio, video, or images. Every form of communication has just the place for steganography as its principles are simple but with lot of security. The concept of steganography deals simply with a cover image, which hides (Karzenbeisser and Perircolas, 2000; Provos and Honeyman, 2003) the secret information in it. The cover being a very common image has a lot of pixel modification being done to it with many randomizations in the bits.

The changed image is now again retrieved back to its original form, but still keeping the bits just in place. This piece of technology has reached ever dreaming heights of security (Marvel *et al.*, 1999) and the end still to be discovered.

The color image steganography (Petitcolas *et al.*, 1999) is a most widely used technique used in the field of information hiding. The steganographic techniques used keeps the existence of the data secret. LSB substitution (Thien and Lin, 2003; Chan and Cheng, 2004; Yang, 2008) is a simple technique in spatial domain steganography .It involves the substitution of least significant bits of the image pixels, by the secret data in binary format.

RSA is an effective algorithm for public-key cryptosystem (Rivest *et al.*, 1978). This is the first cryptoscheme cognized to be worthy for signing as well as encryption and was one of the first groovy advances of public-key cryptoprotocol. A involves key generation, encryption and decryption. The secret data is encrypted (Karzenbeisser and Perircolas, 2000) with a public-key which is known to all. It can only be decrypted by a private key.

The planes in which the data is embedded can be controlled by a technique called the Pixel indicator (Gutub *et al.*, 2008; Gutub, 2010; Amirtharajan and Balaguru, 2009; Amirtharajan *et al.*, 2010a, b, c, 2011, 2012). The pixel indicator technique assigns one of the three planes as the indicator channel and based on the last two bits of the indicator channel the embedding is done in the other two planes. The embedding order in the planes can be changed for increasing the complexity of the algorithm. In this proposed study, the conventional pixel indicator has been changed. If the LSB is 0 the embedding is done in the blue plane and if the LSB is 1 the embedding is done in the green plane.

Sometimes the same image can be used by the different users for embedding their data (Padmaa *et al.*, 2011).

Graphs considered in this paper are simple, tree, finite and undirected. In general G (V, E) denotes the graph G with vertex set V (G) and edge set E (G), such that $|V(G)| = p$, $|E(G)| = q$. A labeling of the vertices of G with the numbers from 0 to q is an injective map $f: V \rightarrow \{0, 1, ..., q\}$. Let $G: E \rightarrow \{1, 2, ..., q\}$ be a bijective. Then a graph G is graceful (Rosa, 1967) introduced as a **β**-valuation), if there exists a labeling of its vertices and edges with the condition for all $u, v \in V(G)$

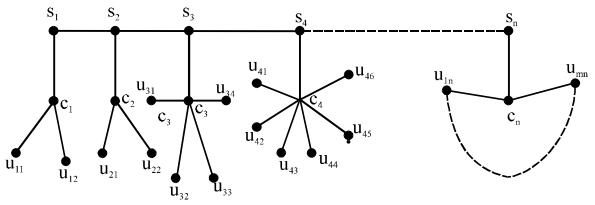

Fig. 1: A Random Tree in which its branches are non decreasing order

with u vϵE (G) such that g (u v) = | f (u)-f (v)|. The same type of analysis by Golomb (1972) is called Graceful labeling. An extensive survey of contributions to graceful labeling of variety of graphs is made (Gallian, 2011).The structure of the graceful labeling is shown in the Fig. 1.

Let $P_n(s_1\text{-}s_2\text{-}\ldots\text{-}s_n)$ be basic path of $T_{S(n)}$ tree. The vertices of the path P_n are also termed as supporting vertices of $T_{S(n)}$ tree. In $T_{S(n)}$ at each s_i, a star S_i hangs with i branches having centre c_i with one of the branch vertices of S_i is merged with s_i. The special tree with hanging stars whose branches satisfy the condition $|E(S_1)| = |E(S_2)| = \ldots = |E(S_n)|$ (non-decreasing number of branches in the hanging stars).

Let $T_{S(n)}$ be a tree with n stars $T_1, T_2, \ldots, T_n$ be stars with $|v(s_i)| = i$ for i = 1, 2, 3,..., n. Free leaves of each of the stars S_i are denoted by u_{im} for i = 1, 2 ,... , n.

Let $T_1, T_2, \ldots, T_n$ be the central values of the stars $S_1, S_2, S_3, \ldots, S_n$ respectively. It can be verified that $|V(T_{s(n)})| = |V(S_1)|+|V(S_2)|+\ldots+|V(S_n)|$ and $|E(T_{s(n)})| = |E(S_1)|+|E(S_2)|+\ldots+|E(S_n)|+(n-1)$.

Let $|E(S_i)| = q_i$ for i = 1, 2, ... , n and $Q= q_1+q_2+\ldots+q_n+(n-1)$. Labeling of vertices in general denoted by l(v):

- $l(s_1) = 0$; $l(c_1) = Q$; $l(c_2) = q_1$ and $l(s_2) = Q-q_1$
- $l(c_{2j+1}) = Q- (\sum_{i=1}^{j} q_{2i} + j)$, j = 1
- $l(c_{2j}) = \sum_{i=0}^{j-1} q_{2i+1} + j - 1$, j = 1.
- $l(s_{2j}) = Q - (\sum_{i=0}^{j-1} q_{2i+1} + j\text{-}1)$, j = 1.
- $l(s_{2j+1}) = \sum_{i=1}^{j} q_{2i} + j$, j = 1

Let the users in growing ith star of $T_{S(i)}$ at s_i be $u_{i1}, u_{i2}, \ldots, u_{in}$.

Let the users in S_1 are labeled with values 1 to q_1-1. Then for i = 1, the labeling of users in odd stars of S_{2i+1} based on its supporting vertex s_{2i+1} as follows:

- Labeling of users in S_{2i+1} is {integers starting from $l(c_{2i})$ + 1 to the number of users in the particular star assigned in ascending order except the value of $l(s_{2i+1})$ }

The labeling of users in even stars S_{2i} based on its supporting vertex s_{2i} as follows.

- Labeling of users in S_{2i} is {integers starting from $l(c_{2i-1})$-1 to the number of users in the particular branch assigned in descending order except the value of $l(s_{2i})$}

The labeling of S_i's in which s_{2i+1}, $i \geq 1$ are increasing order and s_{2i}, $i = 2$ are decreasing order in relation with q.

PROPOSED ALGORITHM

In the conventional Image Steganography (Amirtharajan *et al.*, 2010a-c, 2011, 2012; Janakiraman *et al.*, 2012; Thanikaiselvan *et al.*, 2011) algorithms mostly one user will use one image for his covert communication. In many of the Stego (Karzenbeisser and Perircolas, 2000) applications size of the secret data will be less than that of the size of the carrier (Cover Image). This is equivalent to the wastage of bandwidth in a good communication Padmaa *et al.* (2011) proposed a method, where in embedding of two user's data in the same image with high non linearity which is essential for security.

In this proposed study, a novel method for multi-user embedding is proposed as shown in Fig. 2 and implementation is done for 5 users and has been tabulated.

Secret data of all the users will be first encrypted by using AES and then RSA will be employed which escalates the complexity. A graceful graph (Janakiraman and Sathiamoorthy, 2011) has been used for fixing the randomized order of embedding. Priority in the order of embedding among the five users will be changed during every cycle. This precedence is provided by taking all 120 combinations (5!) which introduces more randomness (Lu *et al.*, 2009; Amirtharajan and Rayappan, 2012a, b; Bandyopadhyay *et al.*, 2008; Schneier, 2007) in the order of embedding.

Complexity has reached to next level by slightly modified PI technique where LSB of the Red Channel will indicate the embedding in the other two channels. This scheme can be effectively employed in Banks, Office, Universities, etc., where resource sharing by multiple users are involved.

Embedding algorithm:

- **Inputs:** Secret data (D_U) from all the 5 users, Coverimage (C) and the number of bits to be embedded in each pixel for all the users (which may differ for one from the other)
- **Output:** Stego image(S) with the entire user's data embedded in it

---

Step 1: Convert the secret data of all the users (D_U) into binary stream

Step 2: Let 'I'=U-1, a variable which decides the pixel position where 'U' denotes the user identity number which can vary from 1-5

Step 3: Do the steps from 4 to 10 for all the U values which range from 1-5:

4. I=I+1

Step 5: Let 'x' = LSB of the Red channel in current pixel

Step 6: If x=1 then embed k bits of current user's data in the Green channel of I'th pixel

Else embed k bits of current user's data in the Blue channel of I'th pixel

Step 7: I=I+24 and repeat steps 4 and 5

Step 8: I=I+18 and do steps 4 and 5 once

Step 9: I=I+12 and repeat steps 4 and 5

10. I=I+6 and repeat steps 4 and 5

Step 11: Take the next combination and go to step 3

Step 12: If embedding is done, store the resultant image as Stego Image(S)

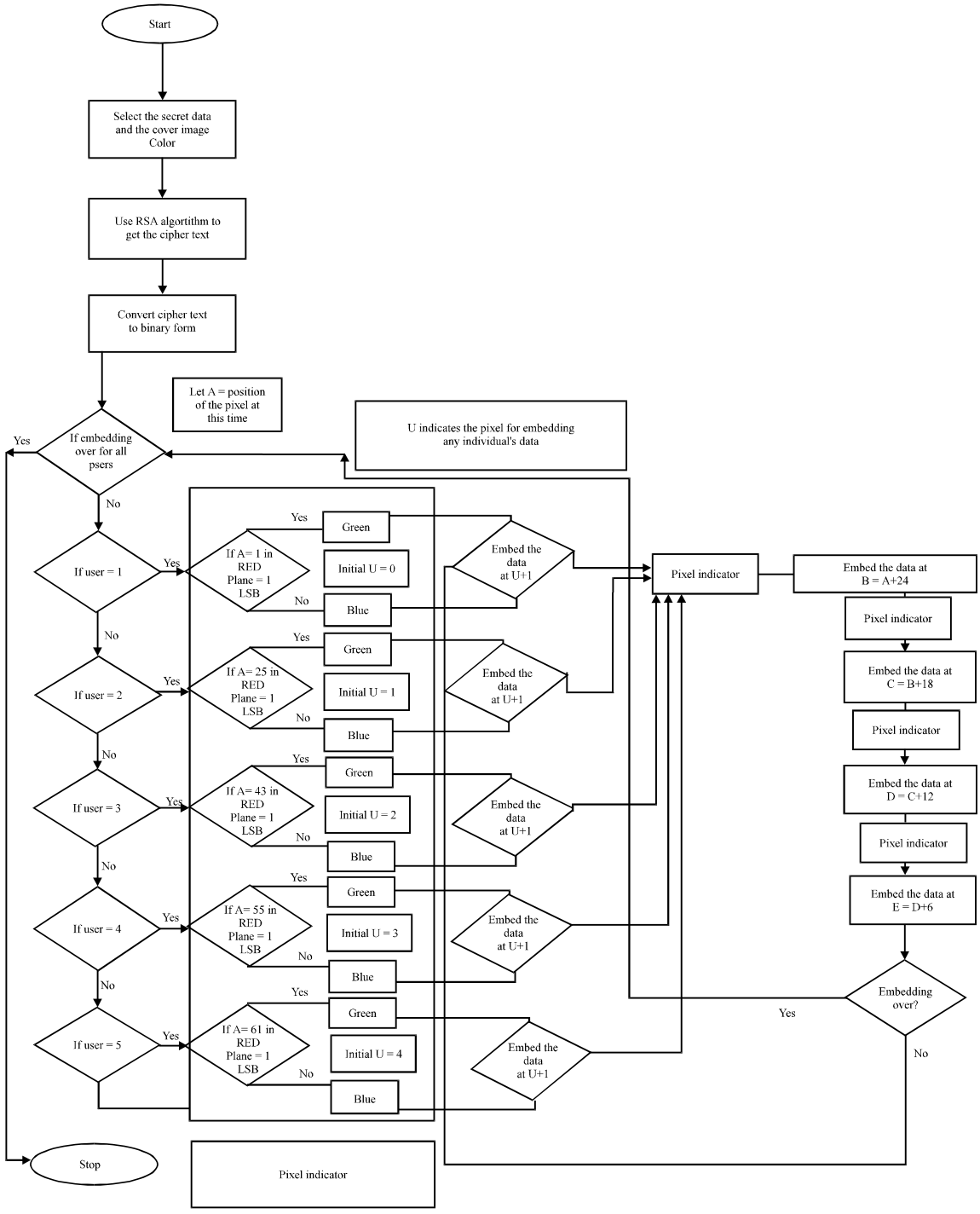

Fig. 2: Flowchart of the proposed methodology

Recovery algorithm:

- **Input:** Stego image(S) with the entire user's data embedded in it
- **Output:** Secret data (D_U) of all the 5 users

Step 1: Let 'I'=U-1, a variable which decides the pixel position where 'U' denotes the user identity number which can vary from 1-5
Step 2: Do the steps from 3 to 9 for all the U values which range from 1-5:
Step 3. I = I+1
Step 4: Let 'x' = LSB of the Red channel in current pixel
Step 5: If x=1 then extract k bits of current user's data from the Green channel of I'th pixel and concatenate to D_U.
Else extract k bits of current user's data in the Blue channel of I'th pixel and concatenate to D_U.
Step 6: I=I+24 and repeat steps 4 and 5
Step 7: I=I+18 and do steps 4 and 5 once
Step 8: I=I+12 and repeat steps 4 and 5
Step 9: I=I+6 and repeat steps 4 and 5
Step 10: Take the next combination and go to step 2
Step 11: Store the recovered Secret data (D_U)

ERROR METRICS

Parameters that are helpful in estimating the standard of the Stego (Sutaone and Khandare, 2008) object are MSE and PSNR. The Mean Square Error is calculated by using the equation:

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

where, $X_{i,j}$ is Stego value and $Y_{i,j}$ is the cover object.

The PSNR is calculated using the Eq.:

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

where, I_{max} is the intensity value of each pixel, which is equal to 255 for 8-bit gray scale images.

Higher the value of PSNR betters the image quality. Here in implementation Tree, Football, Lena and baboon (256×256) color digital images has been taken as cover images and tested for full embedding capacity. The effectiveness of the Stego process proposed has been studied by calculating MSE and PSNR for all the four digital images in RGB planes and displayed in Table 1.

Table 1: Results obtained through number of bits embedded on the respective images

		Channel 1 (Red)		Channel 2 (Green)		Channel 3 (Blue)	
Cover image	No. of bits embedded	MSE	PSNR	MSE	PSNR	MSE	PSNR
Tree	1	0	8	0.0064	70.0666	0.0064	70.0562
	2	0	8	0.0366	62.4965	0.0401	62.0955
	3	0	8	0.1691	55.8485	0.1884	55.3802
	4	0	8	0.4846	51.2770	0.4723	51.3885
Football	1	0	8	0.0063	70.1607	0.0063	70.1431
	2	0	8	0.0348	62.7118	0.0369	62.4640
	3	0	8	0.1624	56.0246	0.1623	56.0267
	4	0	8	0.4552	51.5488	0.4702	51.4081

Table 1: Continue

		Channel 1 (Red)		Channel 2 (Green)		Channel 3 (Blue)	
Cover image	No. of bits embedded	MSE	PSNR	MSE	PSNR	MSE	PSNR
Lena	1	0	8	0.0068	69.7990	0.0060	70.3517
	2	0	8	0.0376	62.3780	0.0346	62.7360
	3	0	8	0.1691	55.8492	0.1595	56.1032
	4	0	8	0.4804	51.3150	0.4296	51.7997
Baboon	1	0	8	0.0061	70.2895	0.0063	70.1431
	2	0	8	0.0354	62.6395	0.0377	62.3675
	3	0	8	0.1625	56.0225	0.1546	56.2374
	4	0	8	0.4753	51.3609	0.4846	51.2773

Fig. 3: Sample images taken as cover images

Fig. 4: Images after processing of stego

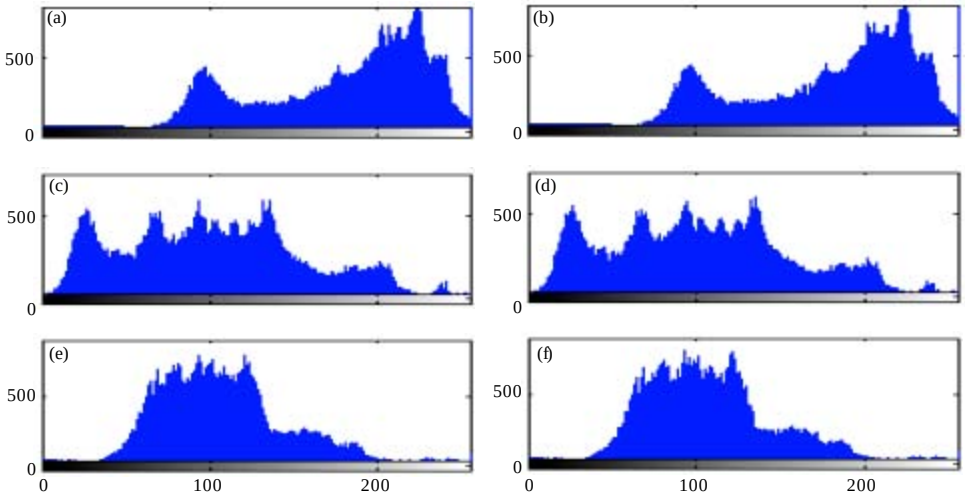

Fig. 5(a-f): k=1 bit embedding users (a) Red plane of cover, (b) Red plane of stego, (c) Green plane of cover, (d) Green plane of stego, (e) Blue plane of cover and (f) Blue plane of stego

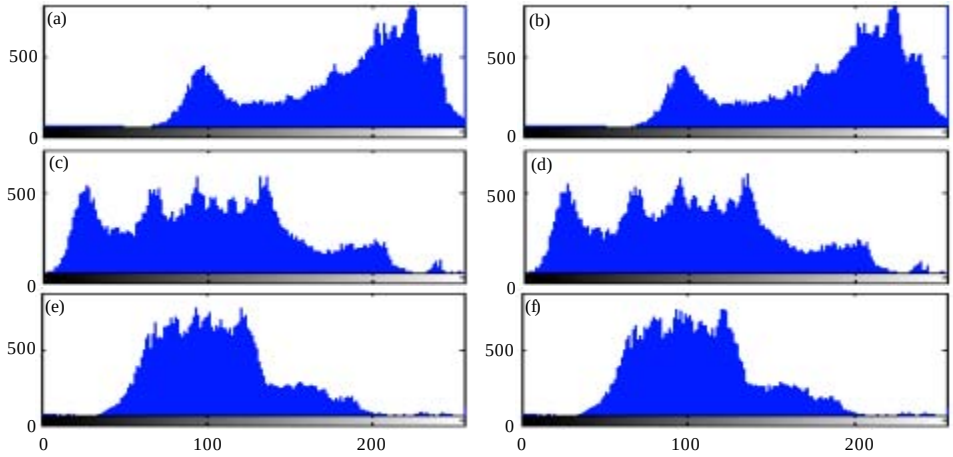

Fig. 6(a-f): k=2 bit embedding for all users, (a) Red plane of cover, (b) Red plane of stego, (c) Green plane of cover, (d) green plane of stego, (e) Blue plane of cover and (f) Blue plane of stego

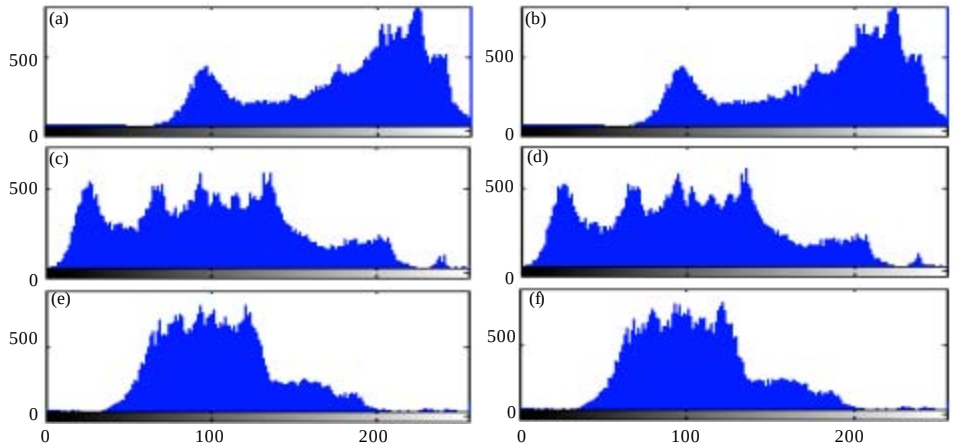

Fig. 7(a-f): k=3 bit embedding for all users, (a) Red plane of cover, (b) Red plane of stego, (c) Green plane of cover, (d) green plane of stego, (e) Blue plane of cover and (f) Blue plane of stego

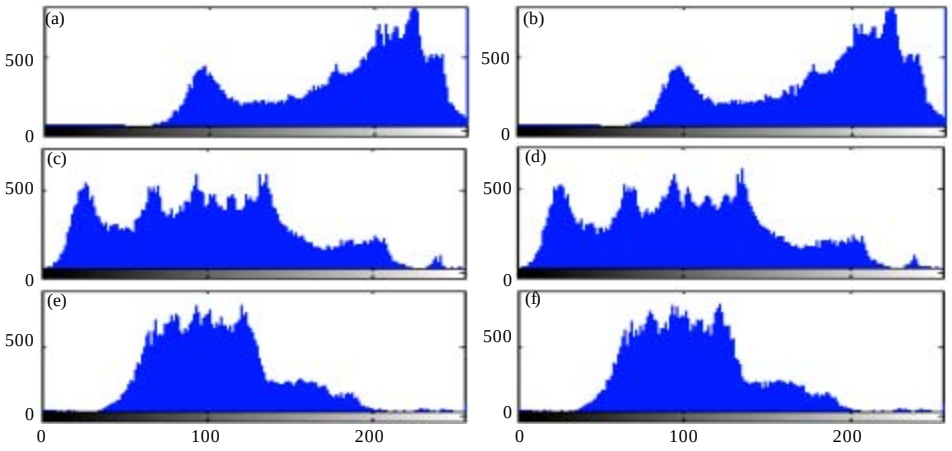

Fig. 8(a-f): k=4 bit embedding for all users, (a) Red plane of cover, (b) Red plane of stego, (c) Green plane of cover, (d) green plane of stego, (e) Blue plane of cover and (f) Blue plane of stego

Figure 3 represents the cover images and Fig. 4 represents the stego image after processing. The following are the histograms that are obtained for k = 1, 2, 3 and 4 bit embedding in Lena image are given in Fig. 5, 6, 7 and 8, respectively.

CONCLUSION

Thus a Multi-user public Cryptic-Stego system has been implemented and data is embedded by using the LSB substitution (Mielikainen, 2006) method. And the randomization introduced by the concept of graceful labeling and the combinational user index in the order of embedding will puzzle the user and even he will not be aware of where his confidential data is hidden inside the carrier. Further the PI technique has been used for increasing the complexity. The data to be embedded is encrypted by Individual users using AES and the use of RSA for the public cryptography provides a two layer security. MSE and PSNR of the Stego image (Gonzalez and Woods, 2002) have been analyzed. From the experimental results given above, the system proves to be a good method and the complexity is increased. This can be applied in places where the resources are shared by many users.

REFERENCES

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

Amirtharajan, R., G. Aishwarya, M. Rameshbabu and J.B.B. Rayappan, 2010b. Optimum pixel and bit location for colour image stego-a distortion resistant approach. Int. J. Comput. Appl., 10: 17-24.

Amirtharajan, R., S.K. Behera, M.A. Swarup, K.M. Ashfaaq and J.B.B. Rayappan, 2010c. Colour guided colour image steganography. Universal J. Comput. Sci. Eng. Technol., 1: 16-23.

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. Inf. Sci., 193: 115-124.

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

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

Bandyopadhyay, S.K., D. Bhattacharyya, D. Ganguly, S. Mukherjee and P. Das, 2008. A secure scheme for image transformation. Proceedings of the 9th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, August 6-8, 2008, Phuket, Thailand, pp: 490-493.

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

Gallian, J.A.A., 2011. A dynamic survey of graceful labeling. Electron. J. Comb.

Golomb, S.W., 1972. How to Number a Graph. In: Graph Theory and Computing, Read, R.C. (Ed.). Academic Press, New York, USA., pp: 23-37.

Gonzalez, R.C. and R.E. Woods, 2002. Digital Image Processing. Prentice Hall, New Jersey.

Gutub, A., M. Ankeer, M. Abu-Ghalioun, A. Shaheen and A. Alvi, 2008. Pixel indicator high capacity technique for RGB image based steganography. Proceedings of the 5th IEEE International Workshop on Signal Processing and its Applications, March 18-20, 2008, Sharjah, UAE.

Gutub, A.A.A., 2010. Pixel indicator technique for RGB image steganography. J. Emerg. Technol. Web Intell., 2: 56-64.

Janakiraman, T.N. and G. Sathiamoorthy, 2011. Graceful labeling of a family of special tree with hanging stars having non-decreasing number of branches in random order. Int. J. Eng. Sci. Adv. Comput. BioTechnol., 2: 130-138.

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

Karzenbeisser, S. and F.A. Perircolas, 2000. Information Hiding Techniques for Steganography and Digital Watermarking. Artech House, UK., ISBN: 9781580530354, Pages: 220.

Lu, T.C., S.R. Liao, P.L. Chen, C.C.C. Chang and Z.H. Wang, 2009. Information hiding technology based on block-segmentation strategy. Proceedings of the ISECS International Colloquium on Computing on Communication, Control and Management, Volume 1, August 8-9, 2009, Sanya, pp: 500-506.

Marvel, L.M., C.G. Boncelet Jr. and C.T. Retter, 1999. Spread spectrum image steganography. IEEE Trans. Image Process., 8: 1075-1083.

Mielikainen, J., 2006. LSB matching revisited. IEEE Signal Process. Lett., 13: 285-287.

Padmaa, M., Y. Venkataramani and R. Amirtharajan, 2011. Stego on 2^n: 1 Platform for users and embedding. Inf. 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.

Rivest, R., A. Shamir and L. Adleman, 1978. Method for obtaining digital signatures and public-key cryptosystems. Commun. ACM, 21: 120-126.

Rosa, A., 1967. On certain valuations of the vertices of a graph. Proceedings of the International Symposium on Theory of Graphs, July, 1966, Rome, Italy, pp: 349-355.

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

Sutaone, M.S. and M.V. Khandare, 2008. Image based steganography using LSB insertion technique. Proceedings of the IET International Conference on Wireless, Mobile and Multimedia Networks, January 11-12, 2008, Mumbai, India, pp: 146-151.

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

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 Recog., 36: 2875-2881.

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