Research Journal of

Information Technology

ISSN 1815-7432

Academic Journals Inc.

www.academicjournals.com

Research Journal of Information Technology 5 (3): 317-328, 2013
ISSN 1815-7432 / DOI: 10.3923/rjit.2013.317.328

Random Abrasion on Image for Security Magnification

[1]Amirtharajan, [2]R. Anushiadevi, [2]V. Meena, [2]V. Kalpana and [1]J.B.B. Rayappan
[1]Department of Electronics and Communcation Engineering, School of Electrical and Electronics Engineering SASTRA University, India
[2]Department of Computer Science Engineering, School of Computing, SASTRA University, India

Corresponding Author: Amirtharajan, Department of Electronics and Communcation Engineering, School of Electrical and Electronics Engineering SASTRA University, India

ABSTRACT
In this study, projected a model for safe secret-digital file transmission by having Steganography as the ground. Steganography, in prehistoric times, dealt with camouflage of secrets between two parties. A part from text, many images, audio and video in millions are shared between millions. All sorts of the aforesaid face a common and serious challenge. Here proposed three routines, in which clandestine information is embedded based on the key in method 1, i.e., number and position of 1s in the four Least Significant Bits (LSB) of the key decides the pixels for embedding. In method 2, position of 1s in the entire key decides the pixels and the position of 1s in four LSBs only decides the location for embedding. In method 3, secret data is plunged by means of the same process but not directly. Instead, it is encoded by Huffman Coding and then embedded. Justification for this study is given by computing Mean Squared Error (MSE) and Peak Signal-to-Noise Ratio (PSNR) values for all the planes in the images by taking sample key values for all the three methods. Experimental results are demonstrated and the corresponding image outputs are also presented.

Key words: Information hiding, symmetric key steganography, huffman coding, key generation

INTRODUCTION
From the famous quote “actions speak louder than words”. Present days communication deals with the means to communicate the human actions directly to others rather than mere words or voices. Technology has been carved into many shapes over the years and will still have potential of a dramatic increase. Communication by actions involves the digital media (Cheddad *et al*., 2010), which is reforming and revolutionizing its dynamism every moment. This growth of the technology in the communication field have plethora of threats that are going to diminish the growth (Stefan and Fabin, 2000). With the birth of technology growth, took birth the hackers who easily hunt for the data and gather by some means. This scared many of the inventors for getting better technology into implementation (Amirtharajan and Rayappan, 2012a, b; Hmood *et al*., 2010a, b; Thenmozhi *et al*., 2012).

Security concerns and threats posed by the hackers are being tackled by algorithms which are capable of completely distorting the information making it practically undiscoverable for any third person. This means of distortion of information is coined cryptography (Schneier, 2007). Encrypting algorithms are the base for this method. They operate on the piece of data and change its complete form and outlook from its root level (the bits).

But Cryptography's encryption policy being too transparent lead many complications (Zaidan *et al*., 2010), as once anyone sees anything distorted; it's evident that something is being hidden. Hence arose, steganography with maximum opaqueness in its hiding methods. A cover that is used in this method has the capability of practically hiding anything like image, video, sound etc (Amirtharajan *et al*., 2012; Al-Frajat *et al*., 2010; Zhu *et al*., 2011) and specialty being the protection of added randomizations from the intruders apart from the source. This has made steganography very popular among masses and is attracting many towards it for further developments. Though having such great security tool, one must not be cautious enough to correctly use it, nor might it end up similar to the September'11 and destruct the mankind for such a tool. Hence this study suggests three methods for random image steganography to improve imperceptibility.

PROPOSED METHODOLOGY

General schematic diagram of the proposed is given in Fig. 1.

Method 1: This method embeds secret data into the pixels as per the key's four LSBs.

If key K = 13[0 0 0 0 1 1 0 1] then embedding should be in the 1st (2^0), 3rd (2^2) and 4th (2^3) LSBs. If key = 5[0 0 0 0 0 1 0 1] then embedding should be in the 1st (2^0), 3rd(2^2) LSBs.

Method 2: It will embed data into the selected pixels based on the key. And also this method will embed data into the selected pixels based on the four LSBs of the Key.

If key K = 173 [1 0 1 0 1 1 0 1] then embedding should be done in the pixels1, 3, 5, 6, 8. This sequence of embedding should be repeated for a block of eight pixels for complete embedding. In a each selected pixel the embedding should be in the 1st (2^0), 3rd (2^2) and 4th (2^3) LSBs. If key K = 165 [1 0 1 0 0 1 0 1] then embedding should be done in the pixels1, 3, 6, 8. This sequence of embedding should be repeated for a block of eight pixels for complete embedding. In each selected pixel the embedding should be in the 1st (2^0), 3rd (2^2) LSBs.

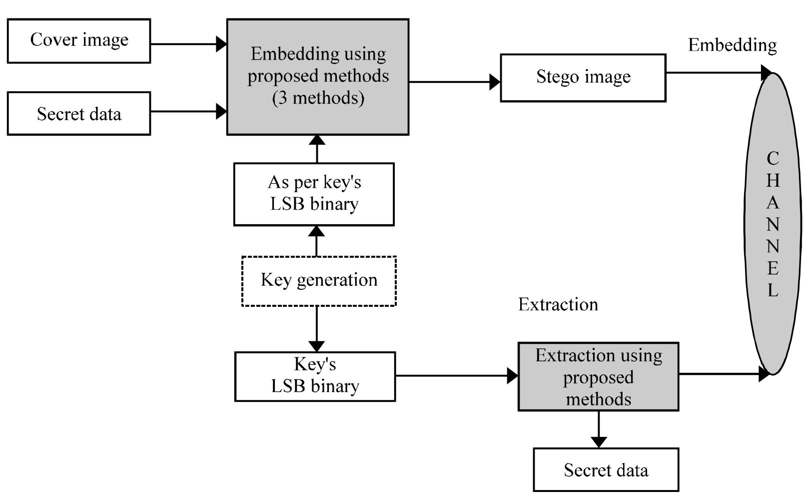

Fig. 1: Block Diagram of proposed system

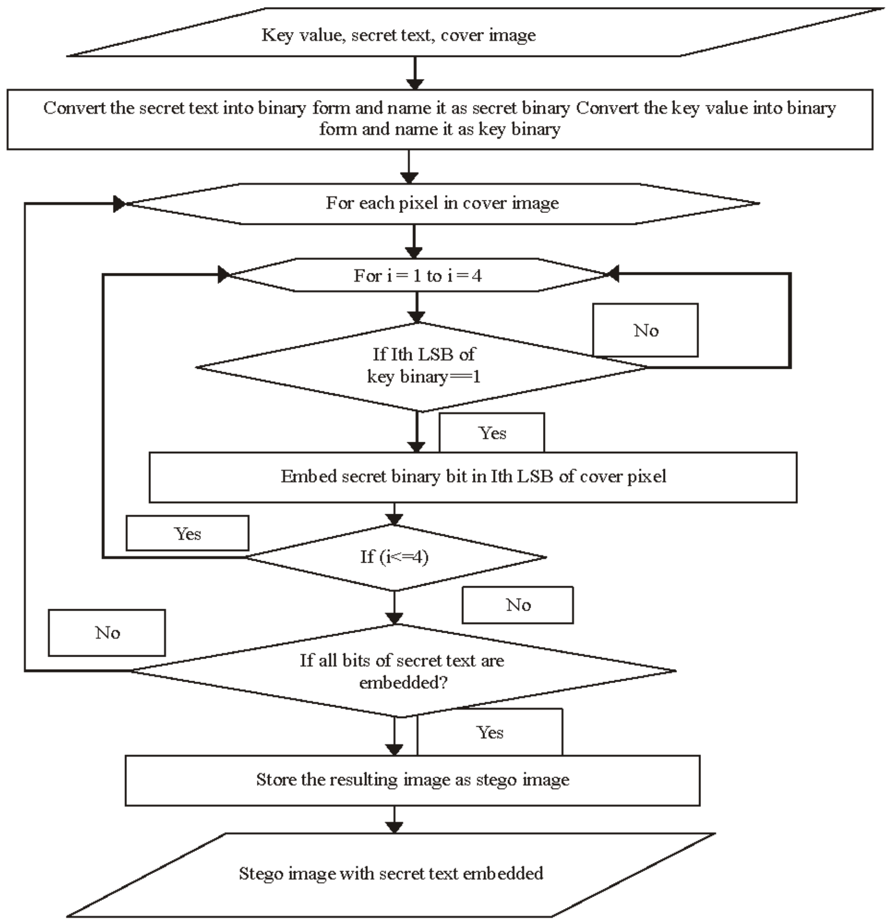

Fig. 2: Flow chart for method 1

Method 3: First data's are embedded using Huffman code then embed encoded data into the selected pixels based on the key. And also this method will embed encoded data into the selected pixels based on the four LSBs of the Key. If key K = 173 [1 0 1 0 1 1 0 1] then embedding should be done in the pixels, 3, 5, 6, 8. This sequence of embedding should be repeated for a block of eight pixels for complete embedding. In a each selected pixel the embedding should be in the 1st (2^0), 3rd(2^2) and 4th(2^3)LSBs. If key K = 165 [1 0 1 0 0 1 0 1] then embedding should be done in the pixels 1, 3, 6, 8. This sequence of embedding should be repeated for a block of eight pixels for complete embedding. In each selected pixel the embedding should be in the 1st (2^0), 3rd (2^2) LSBs.

Algorithms for all three methods are explained below and their corresponding flowcharts are given in Fig. 2-4.

Algorithm for method 1:

Inputs: Secret Data (D), Cover Image(C), key (K)

Output: Stego image(S) with secret data embedded in it.

- Convert the secret text into binary form and name it as secret binary
- Convert the key value into binary form and name it as key binary

Algorithm for method1: Continue

- For each pixel in cover image do the following
  - loop(I = 1 to I = 4)
    - if (Ith LSB of key binary==1)
      embed secret binary bit in Ith LSB of cover pixel
- Store the resulting image as stego image

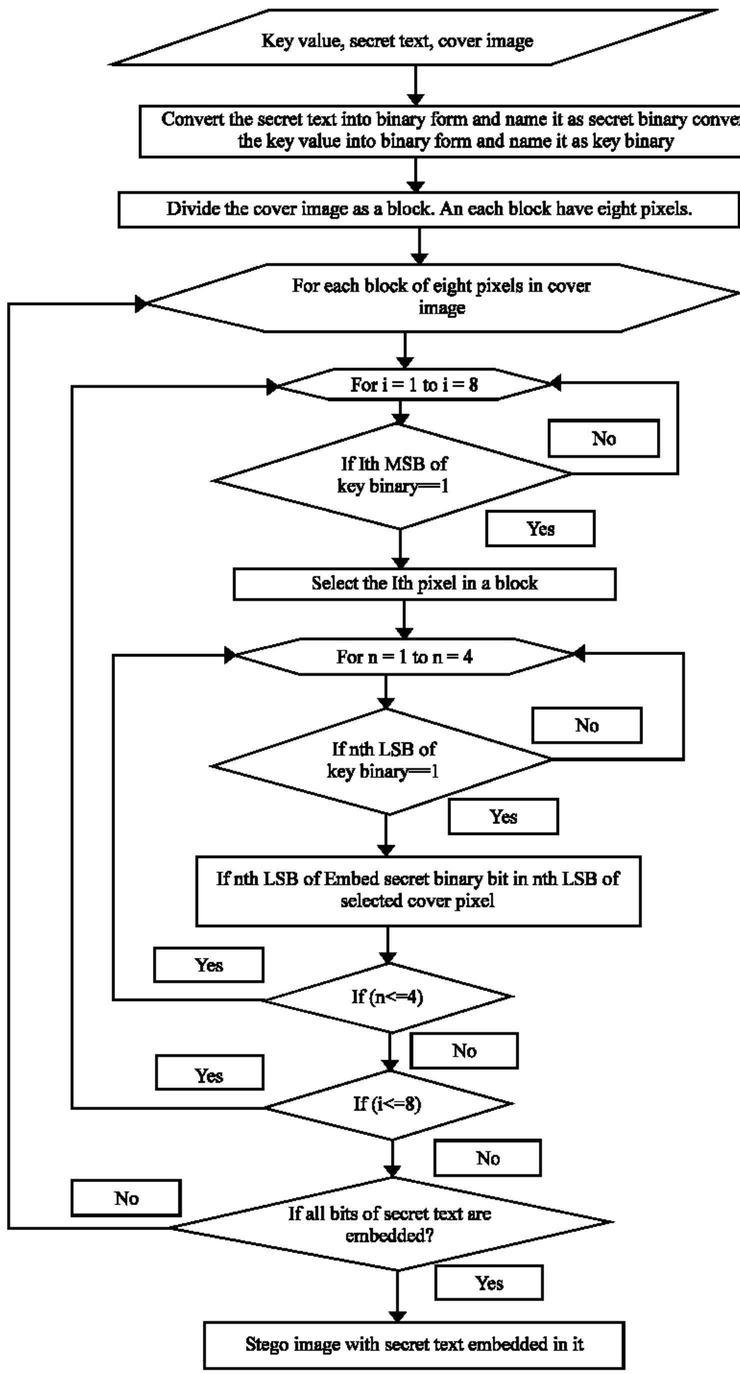

Fig. 3: Flow chart for method 2

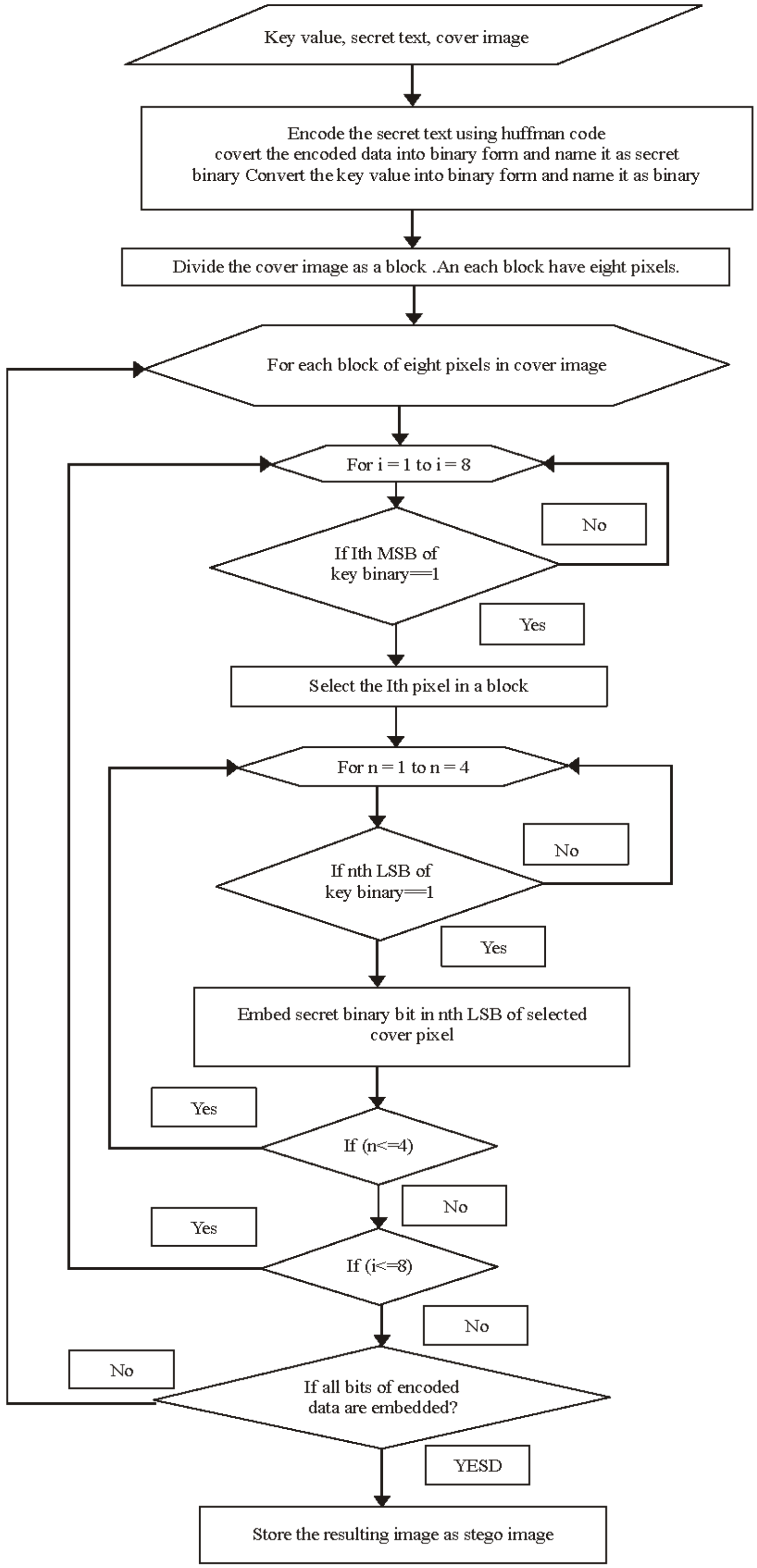

Fig. 4: Flow chart for method 3

Algorithm for method 2:

Inputs: Secret Data (D), Cover Image(C), key (K)

Output: Stego image(S) with secret data embedded in it.

- Convert the secret text into binary form and name it as secret binary.
- Convert the key value into binary form and name it as key binary.
- Divide the cover image as a block. Each block should have eight pixels.
- For each block of eight pixels in cover image do the following
  - Loop (I = 1 to I = 8)
    - if (I^{th} MSB of key binary==1)
    - select the Ith pixel in a block
    - In a selected pixel do the following

      loop(N = 1 to N = 4)

      if (Nth LSB of key binary==1)

      embed secret binary bit in Nth LSB of selected cover pixel
- Store the resulting image as stego image.

Algorithm for method 3:

Inputs: Secret Data (D), Cover Image(C), key (K)

Output: Stego image(S) with secret data embedded in it.

Encode the secret data using Huffman code

- Convert the encoded data into binary form and name it as secret binary.
- Convert the key value into binary form and name it as key binary.
- Divide the cover image as a block. Each block should have eight pixels.
- For each block of eight pixels in cover image do the following
  - Loop (I = 1 to I = 8)
    - if (Ith MSB of key binary==1)
      - select the Ith pixel in a block
    - In a selected pixel do the following

      loop(N = 1 to N = 4)

      if (Nth LSB of key binary==1)

      embed secret binary bit in Nth LSB of selected cover pixel
- Store the resulting image as stego image.

RESULTS AND DISCUSSION

In this study, color images Lena and rose 256×256×3 are taken as covers for the three methods as shown in the Fig. 5a, 6a, 7a, 8a, 9a,10a. For key value of 205, the stego images are given in Fig. 5b, 6b, 7b, 8b, 9b, 10b. The MSE and PSNR values of original and stego images are given in tables. There exist surplus methods for information hiding which aims for robustness, secrecy and imperceptibility. This article swathes all the specifications and boasts that it is steadfast and unswerving when compared with the others.

Method 1 key value = 205 (Fig. 5, 6), Method 2 key value = 205 (Fig. 7, 8) and Method 3 key value = 205 (Fig. 9, 10).

Image quality metrics

Mean squared error (MSE): The average squared difference between a original image and resultant (stego) image is called Mean Squared Error. It dampens small variation between the two pixels but reprimands large ones.

Fig. 5(a-b): Lena (a) Cover image and (b) Stego image

Fig. 6(a-b): Rose (a) Cover image and (b) Stego image

Fig. 7(a-b): Lena (a) Cover image and (b) Stego image

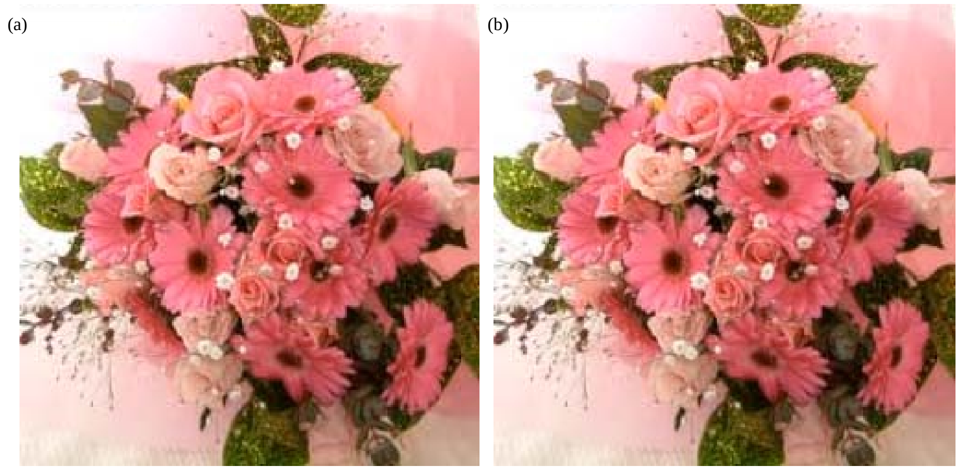

Fig. 8(a-b): Rose (a) Cover image and (b) Stego image

Fig. 9(a-b): Lena (a) Cover image and (b) Stego image

Fig. 10(a-b): Rose (a) Cover image and (b) Stego image

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

where, M and N denote the total number of pixels in the horizontal and the vertical dimensions of the image $C_{i,j}$ represents the pixels in the cover image and $s_{i,j}$ represents the pixels of the stego-image.

Peak signal-to-noise ratio (PSNR): The higher the PSNR, the nearer the stego image is to the cover. A higher PSNR value associates to a high quality image:

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

Table 1 and 2 are the corresponding MSE, PSNR values for method 1
Table 3 and 4 are the corresponding MSE, PSNR values for method 2.

Method 3: First data's are embedded using Huffman code then embed encoded data into the selected pixels based on the key. And also this method will embed encoded data into the selected pixels based on the four LSBs of the Key.

If key K = 173 [1 0 1 0 1 1 0 1] then embedding should be done in the pixels 1, 3, 5, 6, 8. This sequence of embedding should be repeated for a block of eight pixels for complete embedding. In a each selected pixel the embedding should be in the 1st (2^0), 3rd (2^2) and 4th (2^3) LSBs.

Table 5 and 6 gives the corresponding MSE, PSNR values for method 3.

All the stego images give better PSNR (Table 1-6) values for the methodologies and symmetric key plays a major role in retrieval of confidential information.

Table 1: MSE, PSNR values for method 1 for Lena image

			MSE			PSNR		
Pay load size	Cover image	Sample key values	Red	Green	Blue	Red	Green	Blue
1.09 KB	250×250	Key value = 2	0.09945	0.097536	0.09689	58.1544	58.2391	58.2677
		Key value = 4	0.40190	0.390144	0.38860	52.0894	52.2185	52.2356
		Key value = 5	0.23083	0.213792	0.21998	54.4978	54.8308	54.7068
		Key value = 6	0.27987	0.257856	0.25120	53.6612	54.0170	54.1306
		Key value = 8	1.62300	1.509376	1.60460	46.0275	46.3428	46.0771
		Key value = 9	0.91025	0.835488	0.88353	48.5391	48.9114	48.6685
		Key value = 10	0.98028	0.892224	0.93190	48.2172	48.6260	48.4370
		Key value = 11	0.67192	0.590288	0.63328	49.8576	50.4201	50.1148
		Key value = 12	1.23238	1.012480	1.08211	47.2233	48.0769	47.7880
		Key value = 13	0.87704	0.705488	0.77036	48.7006	49.5459	49.2638
		Key value = 14	0.94003	0.746560	0.81529	48.3993	49.4001	49.0176
		Key value = 165	0.23083	0.213792	0.21998	54.4978	54.8308	54.7068
		Key value = 173	0.87704	0.705488	0.77036	48.7006	49.6459	49.2638
		Key value = 205	0.87704	0.705480	0.77036	48.7006	49.6459	49.2638

Table 2: MSE, PSNR values for method 1 for rose image

			MSE			PSNR		
Pay load size	Cover image	Sample key values	Red	Green	Blue	Red	Green	Blue
1.09 KB	250×250	Key value = 2	0.09574	0.09536	0.09696	58.3196	58.3370	58.2640
		Key value = 4	0.38092	0.37939	0.36992	52.3223	52.3399	52.4497
		Key value = 5	0.20728	0.18348	0.19184	54.9652	55.4947	55.3014
		Key value = 6	0.24120	0.19500	0.22105	54.3050	55.2302	54.6857
		Key value = 8	1.54828	1.47251	1.48377	46.2322	46.4502	46.4171
		Key value = 9	0.79108	0.69344	0.74518	49.1485	49.7207	49.4081
		Key value = 10	0.82180	0.73184	0.76531	48.9820	49.4866	49.2924
		Key value = 11	0.57028	0.54356	0.53369	50.5698	50.7782	50.8578
		Key value = 12	1.09360	0.87850	0.99960	47.7420	48.6920	48.1321
		Key value = 13	0.77393	0.65064	0.71417	49.2437	49.9973	49.5927
		Key value = 14	0.80340	0.65996	0.73465	49.0810	49.9355	49.4699
		Key value = 165	0.20720	0.18340	0.19184	54.9650	55.4947	55.3014
		Key value = 173	0.77390	0.65060	0.71417	49.2437	49.9973	49.5927
		Key value = 205	0.77393	0.65060	0.71417	49.2437	49.9973	49.5927

Table 3: MSE, PSNR values for method 2 for Lena image

			MSE			PSNR		
Pay load size	Cover image	Sample key values	Red	Green	Blue	Red	Green	Blue
1.09 KB	250×250	Key value = 2	0.09868	0.096512	0.10041	58.1881	58.2849	58.1127
		Key value = 4	0.39372	0.366336	0.38323	52.1788	52.4920	52.2961
		Key value = 5	0.23012	0.205664	0.21492	54.5111	54.9992	54.8078
		Key value = 6	0.27788	0.236090	0.25267	53.6921	54.3999	54.1052
		Key value = 8	1.60972	1.529856	1.57388	46.0632	46.2842	46.1610
		Key value = 9	0.88190	0.782000	0.81850	48.6764	49.1986	49.0004
		Key value = 10	0.96070	0.827900	0.88400	48.3049	48.9510	48.6661
		Key value = 11	0.67090	0.611200	0.64540	49.8637	50.2689	50.0321
		Key value = 12	1.19140	0.982700	1.02320	47.3701	48.2062	48.0310
		Key value = 13	0.86650	0.729900	0.77606	48.7526	49.4980	49.2318
		Key value = 14	0.94020	0.769700	0.83410	48.3981	49.2674	48.9185
		Key value = 165	0.23614	0.213000	0.21250	54.3990	54.8455	54.8566
		Key value = 173	0.88570	0.684000	0.77990	48.6574	49.7800	49.2102
		Key value = 205	0.87470	0.704500	0.77840	48.7120	49.6515	49.2185

Table 4: MSE, PSNR values for method 2 for rose image

			MSE			PSNR		
Pay load size	Cover image	Sample key values	Red	Green	Blue	Red	Green	Blue
1.09 KB	250×250	Key value = 2	0.09510	0.0992	0.09610	58.3450	58.1628	58.2994
		Key value = 4	0.38118	0.3729	0.38784	52.3194	52.4138	52.2442
		Key value = 5	0.20110	0.1829	0.18350	55.0962	55.5072	55.4935
		Key value = 6	0.23500	0.2145	0.21970	54.4187	54.8146	54.7110
		Key value = 8	1.55230	1.5022	1.53900	46.2208	46.3635	46.2582
		Key value = 9	0.77160	0.7284	0.74880	49.2567	49.5065	49.3871
		Key value = 10	0.80810	0.7633	0.77370	49.0556	49.3036	49.2447
		Key value = 11	0.57640	0.5148	0.53120	50.5233	51.0142	50.8782

Table 4: Continue

			MSE			PSNR		
Pay load size	Cover image	Sample key values	Red	Green	Blue	Red	Green	Blue
		Key value = 12	0.99890	0.8993	1.00680	48.1355	48.5916	48.1011
		Key value = 13	0.74384	0.5976	0.70080	49.4160	50.3660	49.6747
		Key value = 14	0.77950	0.6129	0.72610	49.2121	50.2562	49.5205
		Key value = 165	0.19730	0.1939	0.18890	55.1775	55.2531	55.3678
		Key value = 173	0.77580	0.6232	0.67750	49.2332	50.1841	49.8211
		Key value = 205	0.77040	0.6057	0.68010	49.2630	50.3080	49.8047

Table 5: MSE, PSNR values for method 3 for Lena image

			MSE			PSNR		
Pay load size	Cover image	Sample key values	Red	Green	Blue	Red	Green	Blue
1.09 KB	250×250	Key value = 2	0.05152	0.04953	0.05004	61.0110	61.1815	61.1369
		Key value = 4	0.19328	0.194304	0.19712	55.2689	55.2459	55.1834
		Key value = 5	0.11340	0.115856	0.10875	57.5843	57.4916	57.7664
		Key value = 6	0.14828	0.140992	0.13337	56.4197	56.6388	56.8800
		Key value = 8	0.78848	0.8448	0.77721	49.1628	48.8632	49.2253
		Key value = 9	0.40867	0.390608	0.41651	52.0170	52.2133	51.9345
		Key value = 10	0.45043	0.4208	0.45363	51.5945	51.8900	51.5637
		Key value = 11	0.32524	0.295984	0.33129	53.0086	53.4181	52.9286
		Key value = 12	0.60876	0.516096	0.54758	50.2862	51.0034	50.7462
		Key value = 13	0.39052	0.374032	0.38801	52.2142	52.4017	52.2423
		Key value = 14	0.42124	0.411584	0.42278	51.8854	51.9862	51.8696
		Key value = 165	0.12148	0.108288	0.12128	57.2854	57.7850	57.2929
		Key value = 173	0.43398	0.370256	0.39676	51.7560	52.4457	52.1454
		Key value = 205	0.43862	0.369184	0.39641	51.7098	52.4583	52.1492

Table 6: MSE, PSNR values for method 3 for rose image

			MSE			PSNR		
Pay load size	Cover image	Sample key values	Red	Green	Blue	Red	Green	Blue
1.09 KB	250×250	Key value = 2	0.05050	0.05260	0.0498	61.0927	60.9202	61.1536
		Key value = 4	0.20120	0.20600	0.21555	55.0941	54.9904	54.7952
		Key value = 5	0.11620	0.11130	0.1131	57.4784	57.6635	57.5941
		Key value = 6	0.14140	0.12580	0.1424	56.6250	57.1309	56.5957
		Key value = 8	0.77920	0.85700	0.8386	49.2139	48.8005	48.8949
		Key value = 9	0.42408	0.42752	0.43091	51.8563	51.8212	51.7869
		Key value = 10	0.46750	0.46080	0.46144	51.4328	51.4956	51.4896
		Key value = 11	0.30530	0.30520	0.3025	53.2833	53.2845	53.3226
		Key value = 12	0.60210	0.58850	0.6097	50.3340	50.4330	50.2789
		Key value = 13	0.40430	0.37200	0.39712	52.063	52.424	52.141
		Key value = 14	0.43100	0.39920	0.4055	51.785	52.1178	52.0501
		Key value = 165	0.11228	0.11094	0.11161	57.6274	57.6797	57.653
		Key value = 173	0.43810	0.39480	0.41724	51.714	52.1670	51.9268
		Key value = 205	0.43448	0.39251	0.41582	51.7511	52.1922	51.9417

CONCLUSION

Steganography is the gloomy cousin of cryptography, the use of codes. While cryptography fixes up privacy, steganography is intended to provide secrecy. The focal conventions of a steganographic plot are that it should offer high payload and should be complex enough for the interloper. Selection of pixels and LSB over cover image in order to hide data based on key plays an indispensable role. At the same time, visual artifacts should be nil; this is characterized by PSNR. This study satisfies all these criteria to a greater extent and offers anticipated results and it also transfigure version of other methods. Cover image used in this study helps to improve randomization during the time of embedding secret data; thus it is a type of security all the way through anonymity in view of the fact that no surreptitious data can be rejuvenated without the consent of the keys and coding tactics. The main aim of this study is providing security; security cannot exist in nature, so this study bestows security for confidential data by embedding it in a cover image with the help of this new embedding method. To conclude, this method has philanthropic commercial prospective.

REFERENCES

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 J.B.B. Rayappan, 2012a. 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, 2012b. 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.

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

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.

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

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

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.

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.

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.