Perspectives in Science (2016) 8, 417—420

ScienceDirect
journal homepage: www.elsevier.com/pisc

Adaptive circular queue image steganography with RSA cryptosystem☆

Mamta Jain[a,*], **Saroj Kumar Lenka**[b], **Sunil Kumar Vasistha**[a]

[a] *Department of Computer Science and Engineering, Mody University of Science and Technology, Lakshmangarh, Rajasthan, India*
[b] *Department of Information Technology, Mody University of Science and Technology, Lakshmangarh, Rajasthan, India*

Received 27 January 2016; accepted 9 April 2016
Available online 3 May 2016

KEYWORDS
Circular queue;
Steganography;
Cryptography;
RSA cryptosystem

Summary The major objective of the article is to supply the novel and efficient methodology of digital image steganography that describes individuality regarding secret transmission using the adaptive circular queue least significant bits (LSBs) substitution. The data structure queue is employed dynamically in resource distribution between multiple communication recipients and once secret information transmitted asynchronously. Here, RSA cryptosystem is employed for secret information confidentiality and authentication. The result of the cryptosystem organised into various blocks. In steganography method, organise the cover image into various circular queues blocks. Dynamically adapted procedure is employed to assign secret cypher blocks to circular queues for embedding. Authorised receiver will determine the right plain text using private key in RSA decypherment. Performance analysis is evaluated by using MSE, PSNR and maximum embedding capacity. Results are higher as compared with several of existing algorithms of image steganography.

Introduction

Information and communication technology play a vital appearance now days for implication of lots of IT devices along with security concerns. Sustaining secrecy of electronic data over the World Wide Web in the era of internet, and cloud computing is very crucial aspect. Cryptography and steganography both are used together to accomplish the security challenges to the transmitted data over cloud and mobile networking. Cryptography provides confidentiality to the secret data at end to end communication

☆ This article belongs to the special issue on Engineering and Material Sciences.

* Corresponding author. Tel.: +91 9460981894.
E-mail addresses: mamta11.jain@gmail.com (M. Jain), lenka.sarojkumar@gmail.com (S.K. Lenka), skvasistha.cet@modyuniversity.ac.in (S.K. Vasistha).

http://dx.doi.org/10.1016/j.pisc.2016.04.093

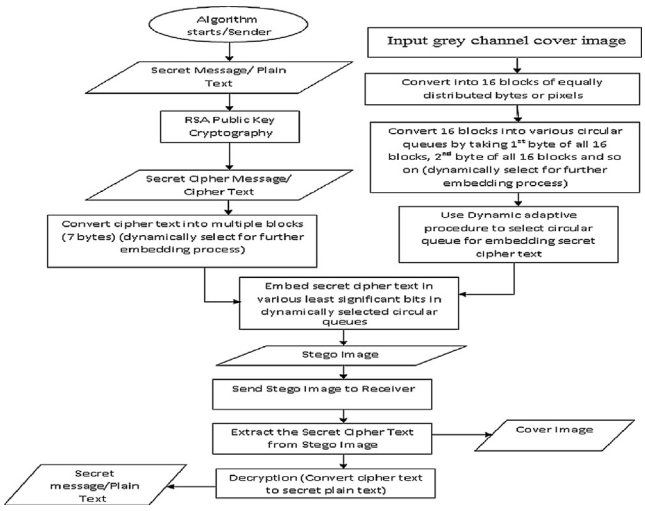

Figure 1 Flow diagram of work methodology.

and data centre for storage. Steganography is a method of secret communication over transmission channel in which secret information is embedded into various multimedia files (Provos and Honeyman, 2003). In steganography, an intruder cannot leak or suspect the secret data that some secret information is passing through transmission channel. The proposed method provides more than one level of security paradigm. Formerly, the data is encrypted using RSA public key cryptography algorithm and later, the encrypted data is concealed into the LSBs of cover image using the circular queue substitutions, thus the strength of steganography can be increased with cryptography. Hiding the data into LSBs of cover image does not much affect its visual appearance quality.

There are numerous procedures used to hide a variety of multimedia secrets inside distinguish multimedia files. Anderson and Petitcolas discussed some limitations in steganography methods. They approached an information theoretic method using Shannon's theory for perfect security of data (Ross et al., 1998). In the another LSB procedure, one bit of secret data is substituted at the 8th position of every byte of the coated file, if the entropy and correlation values of stego image and the cover image show the equality after encyphering then it represents process is safe (Younes and Jantan, 2008). Swain and Lenka (2015) proposed a new steganography technique based on LSB array. One of the four arrays is obtained and formed on the basis of the length of the secret message. The different words of the secret data are mapped on the chosen array, where maximum match found, there obscured the data and start indices are noted down. In the other method, author proposed a two-way block matching procedure and the hop embedding scheme to hide a secret image data inside a cover image (Wang and Chen, 2006). Nag et al. (2011) suggested a novel method in a steganography system based on the affine encryption algorithm and embeds the secret data at the LSB position in order to advise a solid security and imperceptible ocular quality to secret data. Our novel approach can be understood by referring the following divisions. In division 2, the problem formulation and work methodology is suggested, in division 3, results and analysis are done, and finally the work is concluded.

Problem formulation and work methodology

Flow diagram of work methodology

The problem statement consists of circular queue LSB insertion and RSA algorithm to create a secure crypto-stegano algorithm, which is far more secure than many systems being used for the purpose of secretly sending the data. Fig. 1 shows the work flow of this algorithm.

Proposed algorithm

- In our novel opted system, first of all we select a grey image as a cover image and a secret message which will be embedded in the cover image.
- RSA encryption technique is used to encrypt the secret data before embedding.
- After RSA encryption, cypher text will be obtained. Now cypher text will be divided in number of blocks and each block has 7 bytes instead of 8 bytes, since in full circular queue one slot is empty hence one pixel will not used for embedding, it is a property of full circular queue. Now cover image will be divided except some reserved location i.e. to byte numbers 3045—4045 into 16 image blocks and each image block has equal number of bytes or pixels. Now organise the 1st byte of all 16 image block in one circular queue, 2nd byte of all 16 image block in second circular queue and so on. Starting index in circular queue for embedding may be any pixel.
- After that, dynamic adaptive procedure is used for dynamic selection of secret cypher data blocks and circular queue for embedding the secret data and start index for embedding in circular queue. Subtract all the integer values of first data byte of all the data blocks from 255. The data block whose first data byte is having minimum difference value, taken as first data block for processing. After that, all data blocks are taken into consideration based on their difference value in increasing order. Now for dynamic selection of circular queue for data embedding, we take the integer value of all the pixels of second block, which is the second pixel in all the circular queues. Now subtract all the integer values of all pixels of second block from 255. The circular queue whose second pixel is having maximum difference value, taken as first circular queue for data embedding. After that, all circular queues are taken into consideration based on their difference value in decreasing order. For dynamic selection of first embedding index in selected circular queue, we take the starting four bits of first byte of selected secret data block. Now by taking its integer value, we find the start index for embedding in circular queue since in circular queue we can start from any index for performing queue operation.
- Embedding the secret cypher text in cover image using circular queue, is done as follows.
  a. Embed the number of secret cypher message blocks, secret cypher message block length, number of circular queues in cover image, number of circular queues in cover image used for data embedding, length of circular queues, dynamic adaptive procedure generated values for selection of circular queues of cover

image and secret message blocks, start index of each selected circular queue for embedding in some reserved location i.e. to byte numbers 3045–4045.

b. Convert the secret cypher text in various blocks of seven bytes each and cover image in various circular queues of sixteen pixels each.
c. Now by using dynamic adapted procedure, select one block of secret cypher message and assign them to one circular queue of cover image, for embedding.
d. Embedding will be done in dynamically selected circular queues sequentially. First pixel for embedding in circular queue is identified by using dynamically selected start index. Here we can embed only 5th to 8th bit LSB position in a pixel for better visual quality of stego image.
e. Go to step (c). Continue this process until all the cypher data block is not empty and all secret cypher text is not embedded in circular queues sequentially and send resultant stego image to the receiver.

- At receiver side, reverse mechanism is used to extract and decrypt the secret data.

Results and analysis

Resultant simulated outcome using MATLAB for different cover images and their stego images are being displayed in Fig. 2. If histograms are also considered, then there is negligible amount of difference between histogram of original cover image and stego image. Histograms for various original images and their stego images are also shown in Fig. 2.

The PSNR, MSE and maximum embedding capacity values at divergent payloads for different images of various sizes are given in Table 1. PSNR is calculated in decibels (dB). A high quality stego image should aspire for 40 dB and above (Li et al., 2011). PSNR outcome is defined by the mean square error (M.S.E) for two $P \times Q$ monochrome images, Where x as well as y are image coordinates, SG_{xy} (stego image) and CV_{xy} (cover image), one of the images is approved a noisy surmise of the other is defined as:

$$\text{M.S.E} = \frac{1}{PQ}\sum_{x=1}^{P}\sum_{y=1}^{Q}(SG_{xy} - CV_{xy}) \tag{1}$$

$$\text{PSNR} = 10\log_{10}\left\{\frac{CV_{max}^2}{\text{M.S.E}}\right\} \tag{2}$$

where CV_{max} = the maximum 255 pixel value, for 8-bit cover images (Li et al., 2011).

Using Fig. 2, one can observe that there is no visual artefacts with the stego images and histograms, it is looking exactly same as corresponding original cover images. Steganography methods performance can be observed by the three valuable specifications: secrecy, volume/capacity, and visual imperceptibility (Li et al., 2011). Secrecy is used to protect data from unauthenticated attackers or intruders. The hiding capacity should be enough to obscure the data in a cover image. Visual quality of stego image should be like that no one can claim about imperceptibility (Cheddad et al., 2010). Fig. 3 shows the result analysis of proposed algorithm using various performance parameters. Using Table 1, results are analysed. By result analysis, it can be noticed that by increasing the cover image size and decreasing the secret data size PSNR value will be increased up to 83.21 dB and MSE value will be decreased up to 0.0003 as well as maximum embedding capacity is increased up to 37%. So that performance will be high with respect to PSNR, MSE and maximum embedding capacity value. Using Table 2, the comparison of the proposed scheme is shown on the basis of minimum calculated PSNR, embedding capacity and visual imperceptibility with the different algorithms proposed by other researchers. Compared to other algorithms suggested by different experts in this field, our approach is a stronger one and can be used for securing any kind of secret data. Fig. 3 shows the result analysis of proposed algorithm using various performance measure parameters.

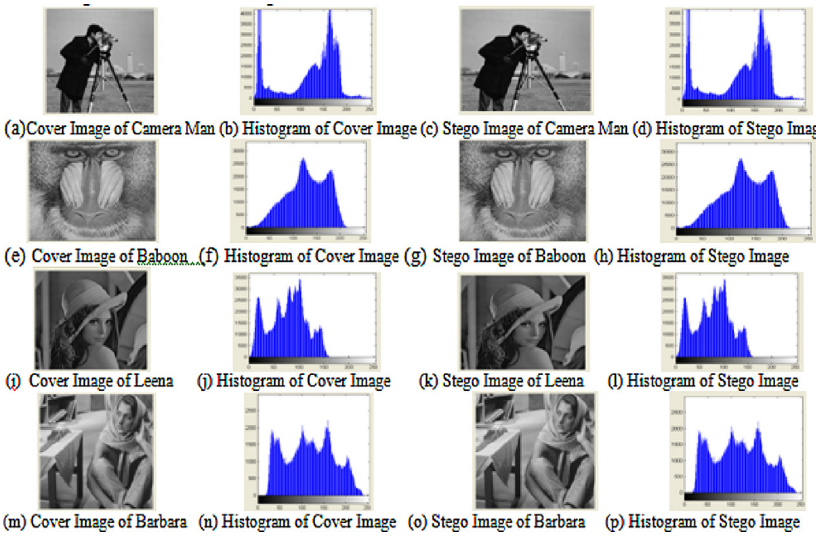

Figure 2 (a), (e), (i), (m) are original cover images and (c), (g), (k), (o) are their stego images respectively, (b), (f), (j), (n) are histograms of original cover images and (d), (h), (l), (p) are their stego images histograms respectively.

Table 1 Observed capacity, MSE and PSNR value (different cover images of same/different size with various secret cypher data of same/different size).

Cover image (*.bmp)	Cover image size (in kilobytes)	Quantity of cypher embedded (in bytes)	Maximum embedding volume (kilo bytes)	Percentage of embedding volume (%) w.r.t (image size)	MSE	PSNR (in dB)
Cameraman	262	256	89.25	34	0.0021	74.71
Cameraman	262	1024	89.25	34	0.0054	70.21
Baboon	262	256	86.61	33	0.0026	73.51
Baboon	262	1024	86.61	33	0.0056	70.61
Leena	262	256	84.23	32	0.0049	72.89
Leena	262	1024	84.23	32	0.0038	70.91
Barbara	262	256	85.67	33	0.0022	75.31
Barbara	262	1024	85.67	33	0.0041	71.46
Cameraman	1048	256	387.03	36	0.0003	83.21
Cameraman	1048	1024	387.03	36	0.0010	78.21
Baboon	1048	256	383.31	37	0.0004	82.03
Baboon	1048	1024	383.31	37	0.0011	77.06
Leena	1048	256	378.04	36	0.0004	82.63
Leena	1048	1024	378.04	36	0.0010	78.52
Barbara	1048	256	380.13	36	0.0003	82.89
Barbara	1048	1024	380.13	36	0.0010	77.53

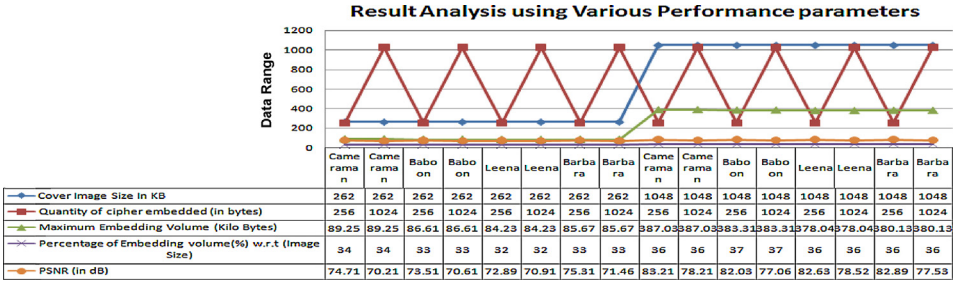

Figure 3 Result analysis of proposed algorithm using various performance parameters.

Table 2 Comparison with other research.

Name of the author and schemes	Minimum calculated PSNR (dB)	Capacity	Visual imperceptibility
Swain and Lenka (2015)	50.50	Good	Better
Wang and Chen (2006)	44.20	Medium	Good
Nag et al. (2011)	30.48	Very low	Poor
Proposed algorithm	70.21	Very good	Best

Conclusion

In this paper, a novel secret transmission scheme is proposed using the notion of obscurity with respect to a circular queue LSBs substitution. The secret message blocks are allocated dynamically by the sender to the image blocks with respect to circular queues, which increases security levels and gives dynamic effect to proposed algorithm. Proposed algorithm uses RSA public key cryptosystem to provide confidentiality of information at data centre end-to-end communication. At steganography level, LSBs substitutions using circular queues are used to protect data from leakage in transmission channel when resources are shared among multiple transmission holders. By result and histogram analysis, it is concluded that PSNR value is better as compared to some of the existing algorithms and imperceptibility distortion cannot be measured from the corresponding stego images.

References

Cheddad, A., et al., 2010. Digital image steganography survey and analysis of current methods. Signal Process. 90, 727–752.

Li, B., et al., 2011. A survey on image steganography and steganalysis. J. Inf. Hiding Multimed. Signal Process. 2 (2), 142–172.

Nag, A., Singh, J.P., Khan, S., Ghosh, S., 2011. A Weighted Location Based LSB Image Steganography Technique, vol. 191. Springer ACC 2011, CCIS 2, pp. 620–627.

Provos, N., Honeyman, P., 2003. Hide and seek: an introduction to steganography. IEEE Secur. Priv. Mag. 1 (3), 32–44.

Anderson, R.J., Petitcolas, F.A., 1998. On the limits of steganography. IEEE J. Sel. Areas Commun. 6 (4), 474–481, Special Issue on Copyright & Privacy protection.

Swain, G., Lenka, S.K., 2015. A novel steganography technique by mapping words with LSB array. Int. J. Signal Imag. Syst. Eng. Indersci. 8 (1–2).

Wang, R.Z., Chen, Y.S., 2006. High payload image steganography using two-way block matching. IEEE Signal Process. Lett. 13 (3), 161–164.

Younes, M.A.B., Jantan, A., 2008. A new steganography approach for image encryption exchange by using the LSB insertion. IJCSNS Int. J. Comput. Sci. Netw. Secur. 8 (6), 247–254.