International Journal of Engineering & Technology, 7 (4) (2018) 3990-3994

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet. v7i4.13713
Research paper

Reversible data hiding in encrypted images with RSA and El gamal algorithm

Chethan R. Bhat [1] *, B. Kishore [1]

[1] Department of Computer Science and Engineering Maniple Institute of Technology Maniple Academy of Higher Education Maniple, Karnataka, India -576104
**Corresponding author E-mail: kishore.b@manipal.edu*

Abstract

This paper puts forward reversible concealing plans for figure content pictures encoded by techniques for open key cryptosystems with probabilistic and homomorphic properties. Inside the reversible plan despite the fact that a direct contortion is presented, the inserted information might be separated, and the special picture might be recuperated from the immediately unscrambled photograph. With the combined strategy, a beneficiary may evacuate a bit of inserted data before unscrambling and expel some other piece of installed data and recuperate the genuine plaintext picture post-decoding. Here we propose to actualize the RSA and ElGamal consolidated calculation for picture encoding and decoding.

Keywords: *Asymmetric Key Encoding, Cryptography; Data Embedding; Image Encoding; Pixel; Reversible Data Hiding.*

1. Introduction

Encoding and information stowing away are two powerful methods for information insurance. While the encoding strategies change over plaintext content into indistinguishable figure message, the information concealing procedures install extra information into cover media by presenting slight adjustments. There are various plans which perform information covering up and encoding together. Distinctive techniques are utilized to conceal the information. Be that as it may, now and again information stowing away in pictures makes harms the first picture and furthermore to the installed information amid extraction. It is possible in the applications like distributed storage and healthcare frameworks.

Being lossless makes this procedure reasonable for medicinal, military applications and distributed storage. In distributed storage, a substance proprietor can scramble a picture to protect his/her security, and transfer the encoded information onto cloud. Circumstances where distributed storage is gotten to by programmer, he will most likely be unable to extricate the information from the scrambled pictures which gives an additional layer of security to the cloud client. Reversible information stowing away in scrambled picture, which can recuperate the first picture with no bending from the stamped picture after the shrouded information have been separated. Present days, reversible information stowing away in encoded pictures is being used because of its brilliant property which is unique cover can be recuperated with no misfortune after extraction of the implanted information [1]. Additionally it secures the first information. Existing Reversible Data Hiding in Encrypted Images (RDHEI) can be separated into two classes: without or with a pre-preparing before picture encoding.

Reversible data hiding was used for authentication. At the beginning stage, reversible calculations had a little installing limit and poor picture quality. While the encoding strategies change over plaintext content into figure message, the information concealing methods implant extra information into cover media by presenting little changes. In some contortion inadmissible cases, information stowing away might be done with lossless or reversible way.

The proprietor of the picture initially scrambles the picture by change, influencing utilization of an encoding to key [2]. The information hider, with no learning about the first picture content, shrouds information into the encoded picture by histogram alteration strategy.

The substance proprietor encodes the first picture [3]. The information hider partitions the scrambled picture into three sets. The beneficiary concentrates message utilizing an extraction key. The rough picture with great quality can be acquired by decoding if only the beneficiary has the unscrambling key. This paper constrains the distortion among three LSB layers and as needs be enhanced the embedding rate.

The work haphazardly chooses pixels from a unique picture to acquire the estimation mistake for mystery information installing [4]. This strategy is first to evaluate a piece of the pixels in a unique picture utilizing the rest pixels and get the estimation mistakes. The information hider then implants the mystery information into the encoded estimation mistakes and scrambles the picture utilizing the sharing key. At the beneficiary side, the mystery information and unique picture can be removed and recouped independently by utilizing diverse security keys.

The creator proposed and assessed another distinct RDHEI structure [5]. A Block Histogram Shifting (BHS) approach utilizing self-shrouded crest pixels is received to perform reversible information inserting. The outcomes exhibit that higher information inserting limit, better decoded checked picture quality, mistake-free information extraction, and precise picture remaking.

Information covering up in the encoded picture is one the protected method for transmission of information safely yet because of specialized angles after extraction there might be enormous misfortune in quality and in addition unique substance of picture [6]. The reversible information concealing methodology expressed as the fundamental undertaking of or work of reversible information concealing calculation is to recuperate unique substance of the scrambled

Copyright © 2018 Chethan R. Bhat, B. Kishore. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

picture [7]. This strategy having a limit of insert high limit information into the picture yet PSNR (Peak Signal to Noise Ratio) must be more noteworthy than 48dB.

The creator proposes the information embedding or information installing procedure in light of LSB strategy [8]. They attempted to recuperate unique substance picture without misfortune, however, this procedure implies that we can state that blend of host flag and the LSB method. To get improved histograms change for reversible information concealing the paper proposes Prediction– Error Expansion (PEE) based reversible information concealing system [9]. The creator utilizes Recursive Code Construction (RCC) and the Rate Distortion Bound (RDB) of reversible information covering up for estimation of RDB and for the excitation of RCC, one should first gauge the Optimal Transition Probability Matrix (OTPM) [10]. Here they propose bound together system bating OTPM for all kind of uses.

In various reversible data covering procedures, an additional place can basically be made open to suit riddle data as long as the picked thing is compressible, yet the points of confinement are not high [11]. Moreover, the payload of this methodology is low since each square can simply convey one piece.

In this paper [12], neighborhood standard deviation of the marked scrambled pictures is examined to evacuate the implanted information amid the unscrambling step. The following proposed [13], receives a superior plan to quantify the piece smoothness. At that point, it utilizes the side-coordinate plan to diminish the mistake rate of extricated bits.

This work proposes Reversible Image Data Hiding (RIDH) plot [14] in the scramble area. An open key tweak system is performed to accomplish information installing, in which access to mystery encoding key isn't required. In [15] the data introducing is done using pixel differentiates; this is an immediate aftereffect of the probability of high redundancies among the neighboring pixel regards in like manner pictures.

The paper [16] proposed the substance proprietor encodes the essential uncompressed picture utilizing an encoding key to make a blended picture. While utilizing both of the encoding and information disguising keys, the presented extra information can be sufficiently cleared and the central picture can be faultlessly recuperated by mishandling the spatial relationship in the typical picture.

2. Methodology

In this area, a consolidated plan of lossless and a reversible information stowing away for open key-encoded pictures is proposed. In the joined plan, the picture supplier performs histogram psychologist and picture encoding. While having the scrambled picture, the information hider may insert the initial segment of extra information. While having the encoded picture, the information hider may implant the initial segment of extra information. On the beneficiary side, the gatherer first focuses the second bit of additional data from the LSB-planes of mixed space. By then, in the wake of deciphering with his private key, he expels the underlying portion of additional data and recovers the principal plaintext picture from the particularly unscrambled picture. The sketch of the proposed scheme appears in Fig. 1.

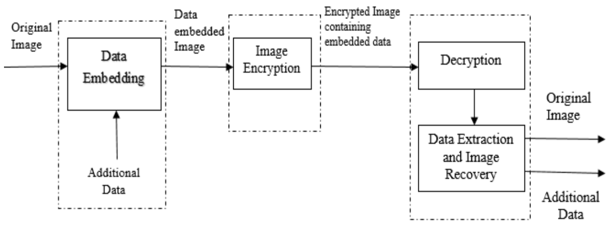


Fig. 1: Reversible Data Hiding Scheme.

However, in [1] for the encoding purpose, Paillier cryptosystem is used. Since RSA consumes less time for encoding and ElGamal takes less time for decoding when compared to Paillier Cryptosystem, replacing this cryptosystem by the combination of ElGamal and RSA algorithm which may result in the reduction in the time required for encoding and decoding process.

RSA is a prominent method out in the public key cryptography. Its security lies in the trouble of figuring huge numbers into prime variables.

The procedure to generate a key pair for encoding is as follows:

1) Select two random prime number, p and q.
2) Compute$r = p \times q$. It should be $p \neq q$, because if $p = q$, then $r = p^2$, and p can be obtained from the square root of r.

$$\text{Compute } \emptyset(r) = (p - 1)(q - 1) \quad (1)$$

3) The select public key PK, which is relatively prime with $\emptyset(r)$.
4) Generate a private keySK.

$$SK.\,PK = 1(\mathrm{mod}(\emptyset(r) \quad (2)$$

The encoding procedure is as follows:

5) The plaintext is separated into squares $x1, x2, \ldots$ with the end goal that every one of the squares speaks to an incentive in the range from0 to $r - 1$.
6) Each block xi is encrypted into the block yi.

$$y_i = x_i^{PK} \mathrm{mod}\ r \quad (3)$$

The decoding procedure is as follows:

Each of the ciphertext blocks is decrypted into the block x_i.

$$xi = yi^{SK} \mathrm{mod}\ r \quad (4)$$

Same as RSA computation, ElGamal is likewise an open key cryptography figuring. This tally was at first utilized for the front-line check, yet afterward, it was adjusted so that it could be utilized for encoding and translating. The idea of this include lies an awful position of figuring discrete logarithm. To scramble and unravel a data embedded, a discrete power is executed. An aggressor that would like to decipher a got message may attempt to recoup the private key. A logarithm should be readied at this side. For this, no true blue framework exists. Under these conditions, the encoding is secure.

The procedures for the generation of a key pair for encoding is as follows:

1) Select a random prime number, p
2) Select two random number g and x, where$(g < p)$and $(x < p)$

$$\text{Compute } y = g^x \bmod p \quad (5)$$

3) x is the private key and y is the public key. The g and p values are public.

The encoding procedure is as follows:

1) Plaintext is isolated into squares $m1, m2, \ldots$ with the end goal that every one of the pieces speaks to an incentive in the range from 0 to $p - 1$.
2) Select a random number, k where $0 \leq k \leq p - 1$, such that k is relatively prime with $p - 1$.
3) Each square of the plaintext m is encoded

$$a = g^k \mathrm{mod}\ p \text{ and } b = y^k \bmod p \quad (6)$$

Pair a, b is figure content for message piece m, so the measure of figure content is double the span of its plaintext.

Decoding of a and b is done by using a secret key x, and plaintext m is recovered by this equation:

$$m = (b/a^x m) \mathrm{mod}\ p \quad (7)$$

Based on the above analysis we can combine both the algorithm by generating the public and private keys via ElGamal algorithm which is given as input to the RSA algorithm for encoding and decoding process. This combined algorithm will reduce the complexity of computation when compared to Paillier cryptosystem.

The procedures for the generation of a key pair for encoding is as follows:

1) Select a random prime number, p
2) Select two random number, g and x, where $(g < p) and\ (x < p)$
3) Compute $y = g^x \, mod \, p$ (8)
4) y is the prime number and its value is public.

The encoding procedure is as follows:

1) Plaintext is organized into the piece m_1, m_2, ... to such an extent that each piece speaks to an incentive in the range from $0 \ to \ r - 1$.
2) Each block m_i is encrypted to block c_i.

$$c_i = m_i{}^x mod \ r \tag{9}$$

The decoding procedure is as follows:

Each cipher text block ci is decrypted into block m_i

$$m_i = c_i{}^y mod \ r \tag{10}$$

Information installing was finished by Wet Paper Coding (WPC) With the encoded picture, the information hider partitions the cipher text pixels into two sets: Set A including $c(i, j)$ with odd estimations of $(i + j)$ and Set B including $c(i, j)$ with even estimations of $(i + j)$. Without loss of sweeping statement, we assume the pixel number Set A is $\frac{N}{2}$. At that point, the information hider utilizes blunder redress codes grow the extra information as a bit succession with length $\frac{N}{2}$ and maps the $\frac{N}{2}$ bits in the coded bit grouping to the cipher text pixels in Set A out of a balanced way. The scrambled picture containing installed information was sent to the beneficiary where he will decode the picture initially took after by extraction of the information.

3. Experimental results and discussion

Grayscale images sized 512×512 Airplane and Baboon were used as original plaintext cover in the experiment and was implemented in MATLAB environment. Both the images used are in PGM format. The PGM format is a lowest common denominator grayscale file format. At the sender side, first the plaintext was embedded in the cover image and then the embedded image was encrypted by the proposed algorithm. The encrypted image after the message was embedded had a PSNR value of 4.20 dB. The encrypted image was then sent to the receiver. At the receiver side, the received image was then decoded. The embedded message was extracted from the decoded image. The decoded image after message extraction was having a PSNR value of 43.28 dB. Fig. 2 and Fig. 4. shows the actual, encoded and decoded images of airplane and baboon respectively. Fig. 3. and Fig. 5. shows the histogram of the actual, encoded and decoded images of airplane and baboob respectively. The time required for encoding process was 0.310768 seconds and for decoding was 8.589123 seconds.

Following table shows the results for proposed plot for airplane and baboon images respectively.

Table 1: Results for Airplane and Baboon Image

Parameter	Airplane	Baboon
Encoding time	0.31 seconds	0.24 seconds
Decoding time	8.58 seconds	7.11 seconds
Encrypted image PSNR	4.20 dB	5.55 dB
Decrypted image PSNR	43.28 dB	41.24 dB

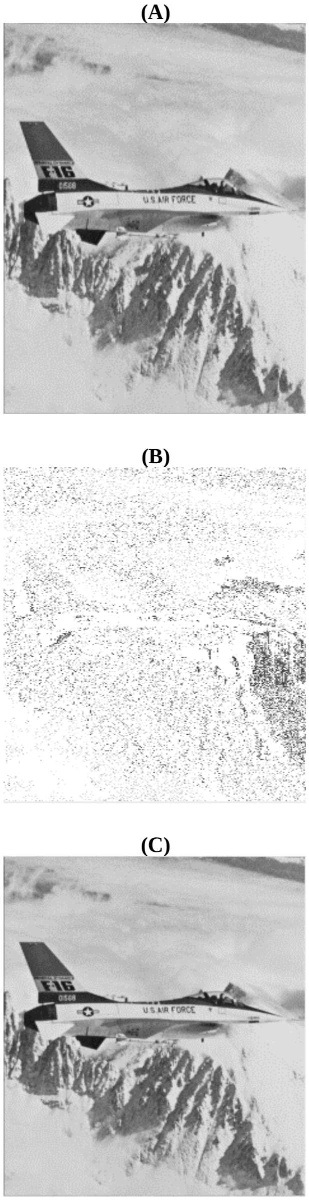
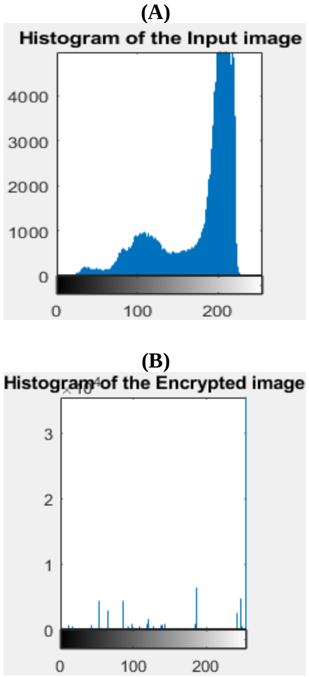

(A)
(B)
(C)

Fig. 2: A) Actual Image B) Encoded Image C) Decoded Image.


(A)

(B)

(C)

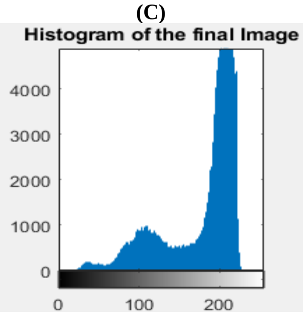


Fig. 3: Histogram of A) Actual Image B) Encoded Image C) Decoded Image.

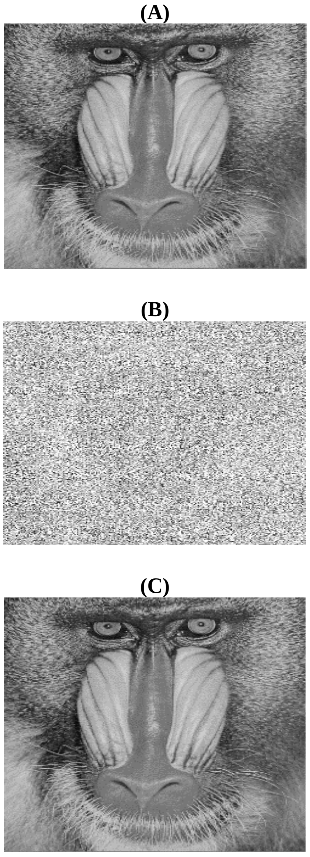
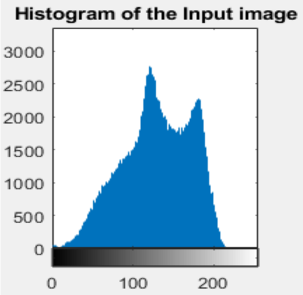
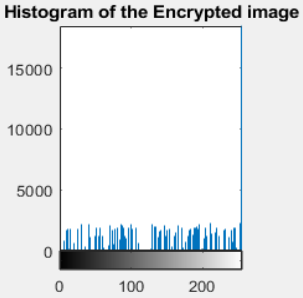


Fig. 4: A) Actual Image B) Encoded Image C) Decoded Image.

(A)



(B)



(C)

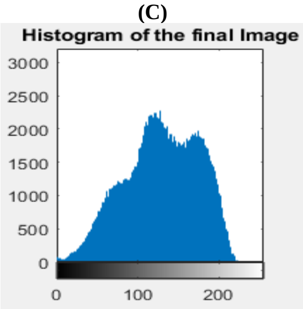


Fig. 5: A) Actual Image B) Encoded Image C) Decoded Image.

Following table shows the comparison of results for encoding schemes proposed in paper [1] and in the current paper.

Table 2: Comparative Analysis for Airplane Image

Parameter	An original method in [1]	Proposed method
Encoding time	8.79 seconds	0.31 seconds
Decoding time	12.65 seconds	8.58 seconds
Encrypted image PSNR	8.51 dB	4.20 dB
Decrypted image PSNR	36.3 dB	43.28 dB

Peak Signal-to-Noise Ratio (PSNR): It characterizes as the proportion of the most extreme conceivable energy of a flag and the energy of debasing commotion that influences the constancy of its portrayal. PSNR is most effortlessly characterized by means of the Mean Squared Error (MSE).

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2 \quad (11)$$

$$PSNR = 20.log_{10}(MAX_I) - 10.log_{10}(MSE) \quad (12)$$

Here, MAX_I is the greatest conceivable pixel estimation of the picture. At the point when the pixels are spoken to utilizing 8 bits for each example, this is 255.

It is observed from Table 2 that the values obtained vary from the values in the other paper and it is noticed that the time taken for the encoding in the proposed plot is less than the plot [1] and time taken for decoding in the proposed scheme is less than plot [1]. However, the total time required for the entire process of the proposed scheme is less than plot [1]. Also, better PSNR value for encrypted and decrypted image is achieved in the proposed plot. In Fig. 3. and Fig. 5., it can be observed in the histogram of the decoded image that there is some loss of pixel information. It is run on MATLAB 2017 with a computer having Intel Core i5 CPU, 4GB RAM, 64-bit processor and operating system used is Microsoft Windows 8.

4. Conclusion and future work

This paper proposes another reversible information concealing plan for ciphertext pictures with a blend of RSA and ElGamal calculation. Security of RSA lies in the trouble of considering expansive numbers into prime components. The proposed calculation, which is a blend of RSA and ElGamal calculation have twofold security. The proposed technique stresses on lessening of time required for encoding and decoding process than on information inserting rate. The proposed strategy has better figuring time when contrasted with different plans. In light of the work that has been done, blend of RSA and ElGamal for encoding has diminished processing time required. Nevertheless, the unscrambling time has not been discretely accomplished. It can be accomplished by doing some investigation in the decoding procedure.

References

[1] X. Zhang, J. Long, Z. Wang, and H. Cheng, "Lossless and Reversible Data Hiding in Encrypted Images With Public-Key Cryptography," in *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 26, no.9, pp.1622-1631, Sept 2016. https://doi.org/10.1109/TCSVT.2015.2433194.

[2] Rintu Jose, and Gincy Abraham, "A Separable Reversible Data Hiding in Encrypted Image with Improved Performance," IEEE International Conference on Microelectronics, Communication and Renewable Energy, Pages: 1-5, 2013. https://doi.org/10.1109/AICERA-ICMiCR.2013.6576038.

[3] Zhenxing Qian, Xinpeng Zhang, and Guorui Feng, "Reversible Data Hiding in Encrypted Images Based on Progressive Recovery", IEEE Signal Processing Letters, Volume: 23, Issue: 11, Pages: 1672-1676, Nov. 2016.

[4] Shuang Yi, and Yicong Zhou, "An Improved Reversible Data Hiding In Encrypted Images," Signal and Information Processing (ChinaSIP) IEEE China Summit and International Conference, Pages: 225-229, 2015. https://doi.org/10.1109/ChinaSIP.2015.7230396.

[5] Zhaoxia Yin, Andrew Abel, Xinpeng Zhan, and Bin Luo, "Reversible Data Hiding In Encrypted Image Based On Block Histogram Shifting," IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Pages: 2129-2133, 2016. https://doi.org/10.1109/ICASSP.2016.7472053.

[6] N. A. Saleh, H. N. Baghdad, S. I. Shaheen, and A. M. Darwish, "High Capacity Lossless Data Embedding Technique for Palette Images Based on Histogram Analysis," *Digital Signal Processing*, 20, pp. 1629−1636, 2010. https://doi.org/10.1016/j.dsp.2010.02.004.

[7] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible Data Hiding," *IEEE Trans. on Circuits and Systems for Video Technology*, 16(3), pp. 354−362, 2006.

[8] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Lossless Generalized-LSB Data Embedding," *IEEE Trans. On Image Processing*, 14(2), pp.253–266, 2005. https://doi.org/10.1109/TIP.2004.840686.

[9] X. Hu, W. Zhang, X. Li, and N. Yu, "Minimum Rate Prediction and Optimized Histograms Modification for Reversible Data Hiding," *IEEE Trans. on Information Forensics and Security*, 10(3), pp. 653-664, 2015. https://doi.org/10.1109/TIFS.2015.2392556.

[10] W. Zhang, X. Hu, X. Li, and N. Yu, "Optimal Transition Probability of Reversible Data Hiding for General Distortion Metrics and Its Applications," *IEEE Trans. on Image Processing*, 24(1), pp. 294-304, 2015. https://doi.org/10.1109/TIP.2014.2358881.

[11] X. Zhang, "Reversible data hiding with optimal value transfer," *IEEE Trans. Multimedia*, vol. 15, no. 2, pp. 316–325, Feb. 2013 https://doi.org/10.1109/TMM.2012.2229262.

[12] W. Puech, M. Chaumont, and O. Strauss, "A reversible data hiding Method for encrypted images," in *Proc. of SPIE 6819*, pp.1-9, 2008.

[13] T. Hong, W. Chen, and H. Wu, "An improved reversible data hiding in encrypted images using side match, " *IEEE Signal Processing Lett.*, vol.19, no.4, pp.199-202, 2012. https://doi.org/10.1109/LSP.2012.2187334

[14] Jiantao Zhou, Weiwei Sun, Li Dong, Xianming Liu, Oscar C. Au Yuan Yan Tang, "Secure Reversible Image Data Hiding over Encrypted Domain via Key Modulation," *IEEE Trans. On* Circuits and Systems for Video Technology, vol. 26, issue 3, pp.441-452, 2015.

[15] Jun Tian, "Reversible data embedding using a difference expansion," in *IEEE Transactions on Circuits and Systems for Video Technology*, vol.13, no.8, pp.890-896, Aug.2003. https://doi.org/10.1109/TCSVT.2003.815962.

[16] X. Zhang, "Separable reversible data hiding in encrypted image," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 826–832, Apr. 2012. https://doi.org/10.1109/TIFS.2011.2176120.