



Stashing Scope Afore Encoding For Revocable Data Spanking In Encoded Images

Dasari Nagaraju #1, Alahari Hanumat Prasad #2

#1 Student of M.Tech Department Of Computer Science Engineering G.V.R&S College of Engineering & Technology, GUNTUR

#2 Department of Computer Science Engineering G.V.R&S College of Engineering & Technology, GUNTUR

ABSTRACT:

Nowadays, information is rapidly available through the Internet. Companies have the ability to communicate with a worldwide audience through the World Wide Web. The extraction is performed in the reverse order as the embedding process. The side information (peak/zero points) should be additionally transmitted to the receiver for reversible recovery. The original cover can be losslessly restored after the embedded information is extracted. In some applications, even any degradation of the original cover is not allowed, such as medical imagery, military imagery and law forensics. All early methods embed assemblage by reversibly vacating space from the encrypted reflections, which may be thing to both errors on data extraction and or appearance refurbishment. Data hacking is very challenging problem in today's internet world. There are number of techniques to secure the data. So, the data hiding in the encrypted reflection comes into the picture, but occurrence of distortion at the time of data extraction is a main problem. In this article, Due to the modification on the pixel differences to hide secret data, the marked differences may be not in the normal range [0, 255] for a 8-bit gray scale image.

I. INTRODUCTION

Most hospitals have already established the electronic medical information to make healthcare better, safer, and more efficient. Over the Internet, digitized medical information is very convenient to transmit among patients, medical professionals, health care providers, and institutes of medicine. Data hiding plays an important role in information security such as authentication, fingerprinting, copy control, security, and covert communication. Reversible data

hiding, which is also called lossless data hiding. Reversible data hiding techniques can be classed into three groups: data compression (VQ), pixel-value difference expansion (DE), histogram-based scheme

legitimate a rate-distortion forge for RDH, through which they proved the rate falsification extent of RDH for memory less conceal and exposed a recursive cipher cerebation which, nonetheless, does not approximate the extent. Zhang et al [2], [3] improved the recursive cipher cerebation for binary conceal and proved that this cerebation can succeeded the rate-falsification extent as elongate as the shrinkage algorithm reaches entropy, which establishes the equivalence between the data shrinkage and RDH for binary conceal. algorithm that not only guarantees the restricted data will be extracted accurately but also allows the original cover reflection to be reconstructed without distortion after the restricted data are completely extracted. This important technique is widely used in medical reflationary, military reflationary and law forensics, where no distortion of the original cover is allowed. The proposed method can achieve real reversibility, that is, data extraction and reflection finding are free of any error. Data hiding process involve two sets of data, 1. A set of the embedded data 2. A set of the cover media data. As when data is embedded into the reflection then the quality of reflection get disturbed. So it is expected that after the data extraction the reflection quality should be maintained just like the original reflection. With regard of distortion in reflection, Kalker and Willems [1] established a rate-distortion copy for RDH. RDH in reflections is a technique, due to which the original cover can be loss less recovered after the Embedded message is extracted. This important technique is widely used in

medical reflationary, military reflationary and law forensics, where no distortion of the original cover is allowed which can be achieved using RDH.

II. WHAT IS RDH (REVERSIBLE DATA HIDING?) Reversible data hiding is a procedure to embed extra message into some distortion-unacceptable cover media, such as military or medical reflections, with a reversible behavior so that the original cover content can be flawlessly restored. In [16], Zhang divided the encrypted reflection into several blocks. By flipping 3 LSBs of the half of pixels in each block, room can be vacated for the embedded bit. The data extraction and reflectionfinding proceed by finding which part has been flipped in one block. This process can be realized with the help of spatial correlation in decrypted reflection. Hong et al. [17] ameliorated Zhang's method at the decoder side by further exploiting the spatial correlation using a different estimation equation and side match technique to achieve much lower error rate. These two methods mentioned above rely on spatial correlation of original reflection to extract data. That is, the encrypted reflection should be decrypted first before data extraction. To separate the data extraction from reflection decryption, Zhang [18] emptied out space for data embedding following the idea of compressing encrypted reflections [14], [15]. Compression of encrypted data can be formulated as source coding with side information at the decoder [14], in which the typical method is to generate the compressed data in lossless manner by exploiting the syndromes of parity-check matrix of channel codes. The method in [18] compressed the encrypted LSBs to vacate room for additional data by finding syndromes of a parity-check matrix, and the side information used at the receiver side is also the spatial correlation of decrypted reflections. All the three methods try to vacate room from the encrypted reflections directly. However, since the entropy of encrypted reflections has been maximized, these techniques can only achieve small payloads [16], [17] or generate marked reflection with poor quality for large payload [18] and all of them are subject to some error rates on data extraction and/or reflection restoration. Although the methods in [16], [17] can eliminate errors by error correcting codes, the pure payloads will be further consumed. In the present paper, we propose a novel method for RDH in encrypted reflections, for which we do not "vacate room after encryption" as done in [16]–[18], but "reserve room before encryption".

III. PROPOSED SCHEME

As we know lossless vacating rooms from the encrypted reflections is comparatively intricate and at times unproductive, why are we still so fanatical to discover novel RDH techniques running directly for encrypted reflections? Imagine if we reverse the order of encryption and vacating room, i.e., reserving room prior to reflection encryption at content owner side. The RDH tasks in encrypted reflections would be more natural and much easier which guide us to the novel framework, "reserving room before encryption (RRBE)". As shown in Fig. 1(b), the content owner first reserves adequate space on original reflection. Then translate the reflection into its encrypted version with the encryption key. Now, the data embedding process in encrypted reflections is essentially reversible. Data hider only needs to have room for data into the spare space previous emptied out. The data extraction and reflectionfinding are indistinguishable to that of Framework VRAE. Noticeably, standard RDH algorithms are the best operator for reserving room before encryption. This can be effortlessly applied to Framework RRBE to realize better performance compared with techniques from Framework VRAE. Reason is, in this new framework, we pursue the customary idea that first losslessly compresses the unneeded reflection content (e.g., using excellent RDH techniques) and then encrypts it with respect to protecting privacy. In the proposed method (Fig 1(b)),

1. We first empty out room by embedding LSBs of some pixels into other pixels with a traditional RDH method.
2. Then encrypt the reflection, so the positions of these LSBs in the encrypted reflection can be used to embed data. This proposed method does below:-
 1. Separate data extraction from reflection decryption
 2. Achieves excellent performance in two different prospects:
 - a. Real reversibility is realized, that is, data extraction and reflectionfinding are free of any error.
 - b. For given embedding rates, the PSNRs of decrypted reflection containing the embedded data are significantly improved; and for the acceptable PSNR, the range of embedding rates is significantly enlarged.

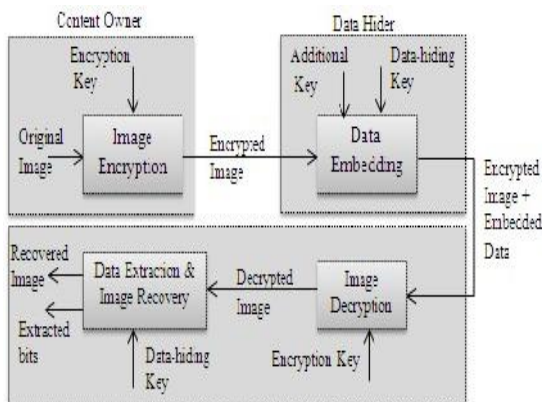


Fig. 1. Framework: “vacating room after encryption (VRAE)” versus framework: “reserving room before encryption (RRBE).”

A. Reflection Encryption Assuming original colorreflection size is $N1 * N2$ and each pixel of Red, green, blue value falling into $[0,255]$ is represented by 8 bits. Denote each bits of a pixel represented as $b_{j,k,0}, b_{j,k,1}, \dots, b_{j,k,7}$ where $1 \leq j \leq N1$ and $1 \leq k \leq N2$, and the rgb value as $q_{j,k}$. Denote the other number of pixels as $N(N=N1 * N2)$. $B_{j,k,a} = [q_{j,k,a} / 2^a] \text{ mod } 2, a=0,1,\dots,7$ (1) and $q_{j,k} = \lfloor 2^a B_{j,k,a} \rfloor$ (2) $B_{j,k,a} = b_{j,k,a} + r_{j,k,a}$ (3) In encryption phase original bits and pseudo-random bits are calculated by exclusive-or. Where $r_{j,k,a}$ are determined by an encryption key using a standard stream cipher.

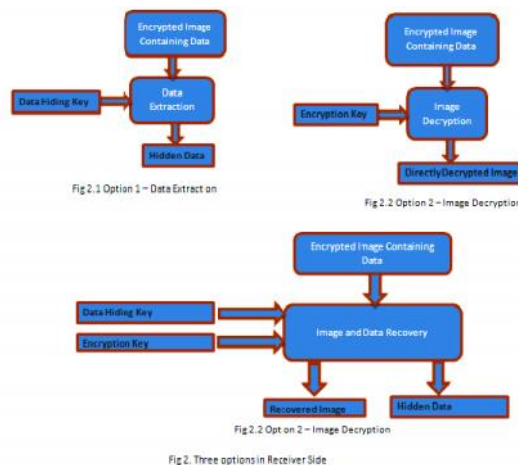
B. Data Embedding

In the data embedding, some parameters D,H,R are embedded into a small number of encrypted pixels, and the other encrypted pixels of LSB are compressed to creating a sparse space for accommodating the additional data. The detailed procedure is as follows. After encrypting the original colorreflection content owner pseudo-randomly selects Nt encrypted pixels according to a data hiding key that will be used to carry the parameters (D,H,R) for data hiding. Here, Nt is a small positive integer. The other $N-Nt$ encrypted pixels are pseudo-randomly permuted and divided into a number of groups using data hiding key, each group contains no of pixels which is denoted as H . Collect the D least significant bits of the H pixels in each group, which is denoted by $B(g,1), B(g,2), \dots, B(g,D,H)$ where g is a group index within $[1, (N-Nt)/H]$ and D is a positive

integer less than 5. Here, S is a small positive integer. The content owner generates a M matrix which has two parts by (4). $M = [ID.H-R \ F]$ (4) Where $ID.H-R$ is an identity matrix $ID.H-R = (D.H-R) \times (D.H-R)$ and $F = (D.H-R) \times R$ which is derived from the data-hiding key. Then, The parameters D,H , and R are embedded into the LSB of Nt . For example if $Nt=16$ the values of D,H and R are represented as 2, 12 and 2 bits respectively, and Nt LSB encrypted pixels replaced by 16 bits. In following, a total bits made up of Nt and $(N-Nt).R/H-Nt$ additional bits will be embedded into the pixel groups. For each group, calculate =

$$\begin{matrix}
 B'(g,1) & & B'(g,1) \\
 \dots & & \dots \\
 B'(g,D.H-R) & & B'(g,D.H)
 \end{matrix} = F \quad (5)$$

C. Data Extraction and Reflection Recover In this phase, there are three options at the receiver side;



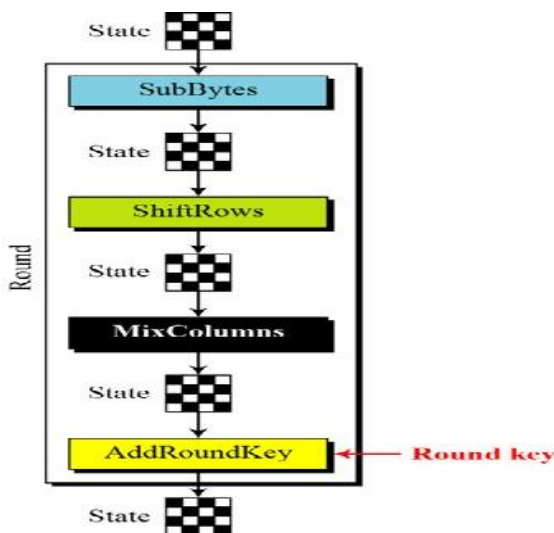
III.AES ALGORITHM

In our system we are using 128 bit key and in AES this is represented by $Nb = 4$, which reflects the number of 32-bit words (number of columns) in the State.

The length of the Cipher Key, K , is 128. The key length is represented by $Nk = 4, 6, \text{ or } 8$, which reflects the number of 32-bit words (number of columns) in the Cipher Key [7]. The number of rounds to be performed during the execution of the algorithm is dependent on the key size. The number of rounds is represented by Nr , where $Nr = 10$ when $Nk = 4$, $Nr = 12$ when $Nk = 6$, and $Nr = 14$ when $Nk = 8$.

For both its Cipher and Inverse Cipher, the AES algorithm uses a round function that is composed of four different byte-oriented transformations:

- 1) Substitution using a substitution table (S-box).
- 2) Shifting rows of the State array by different offsets
- 3) Mixing the data within each column of the State array
- 4) Adding a Round Key to the State. [6].



IV. FUTURE SCOPE

The future implementation is to add support to hide all file formats. This allows for a much broader spectrum of usage: one would be able to encode .exe, .doc, .pdf, .mp3, etc. The system would be more versatile because often hiding text just isn't enough. We can also implement batch reflection processing and statistical analysis so that the system could run the code through a dataset of reflections and detect Steganography and perhaps crawl through Google

Reflection Search to see how prevalent Steganography is.

A. Three Keys For More Data Security

Encrypted data is hidden in Encrypted Reflection with separate keys for Data Encryption, Data Hiding and Reflection Encryption. For decrypting of data receiver should have both Data Encryption and Data hiding key.

B. Protection For Auto Generated Keys

To perform any operation the user has only 3 attempts. If user is fail to perform any of operation

means user enter wrong 3 times then the system is goes to not responding state and one mail with receiver computer IP address is send to the admin.

C. User Define Extension Prevent Hacker Attack

During data hiding process user has to give the extension like .xyz.

D. Admin as Main

Admin of system have all authority that is admin can block, unblock any user at any time if he feel something wrong and admin have all records from all user.

V. CONCLUSION

Reversible data hiding in encrypted reflections is a new topic drawing attention because of the privacy-preserving requirements from cloud data management. Previous methods implement RDH in encrypted reflections by memory space after encryption, as opposed to which we proposed by reserving memory space before encryption. Our study helps constructing secure transmission of secrete file preventing any third party access and security level of data is increased by encrypting data. We also provide protection for keys during decryption process if any hacker attacks on system. In future we can use audio, video in case of reflection as cover for hiding the data.

REFERENCES

- [1] M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, "On compressing encrypted data," *IEEE Trans. Signal Process.*, vol. 52, no.10, pp. 2992-3006, Oct. 2004.
- [2] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 16, no. 3, pp. 354-362, Mar.2006.
- [3] C.-C. Chang, C.-C.Lin, and Y.-H. Chen, "Reversible data-embedding scheme using differences between original and predicted pixel values," *IET Inform. Security*, vol. 2, no. 2, pp.35-46, 2008.
- [4] T. Bianchi, A. Piva, and M. Barni, "On the implementation of the discrete Fourier transform in the encrypted domain," *IEEE Trans. Inform. Forensics Security*, vol. 4, no. 1, pp. 86-97, Feb. 2009.
- [5] W. Liu, W. Zeng, L. Dong, and Q. Yao, "Efficient compression of encrypted gray scale reflections," *IEEE Trans. Reflection Process.*, vol. 19, no. 4, pp. 1097-1102, Apr. 2010.
- [6] T. Bianchi, A. Piva, and M. Barni, "Composite signal representation for fast and storage-

efficient processing of encrypted signals," IEEE Trans. Inform. Forensics Security, vol. 5, no. 1, p. 180-187, Feb. 2010.

- [7] X. Zhang, "Lossy compression and iterative reconstruction for encrypted reflection," IEEE Trans. Inform. Forensics Security, vol. 6, no.1, pp. 53-58, Feb. 2011.
- [8] Xinpeng Zhang "Separable Reversible Data Hiding in Encrypted Reflection" IEEE Trans. VOL. 7, no. 2, Apr 2012.

AUTHORS:



DASARI NAGARAJU is a student of computer science engineering from G.V.R&S College of engineering & technology, presently pursuing M.TECH (cse) from this college. She received B.Tech from JNTUK in

the year of 2008.



ALAHARI HANUMAT PRASAD is a ASSOCIATE PROFESSOR Department of CSE at G.V.R&S college of Engineering & Technology, Guntur. He received M.Tech in Computer science engineering from JNTUK. He gained 10 years Experience on Teaching. He is a good Researcher in Network Security.