Reversible Data Hiding in Encrypted Images using RC4 Algorithm

Ganesh Satras[1] Vivek Bhosale[2] Ajit Gaikwad[3] Shahid Pathan[4]

[1,2,3,4]Department of Computer Engineering

[1,2,3,4]IOK College of Engineering, Pune-412 208

Abstract— The methods proposed can be summarized as the framework, “vacating room after encryption (VRAE)”. In this framework, a content owner encrypts the image using a standard cipher with an encryption key. After producing the encrypted image, the content owner hands over it to a data hider and the data hider can embed some auxiliary data into the encrypted image by lossless vacating some room according to a data hiding key. Then a receiver, maybe the content owner himself or an authorized third party can extract the embedded data with the data hiding key and further recover the original image from the encrypted version according to the encryption key. With regard to providing confidentiality for images, encryption is an effective and popular means as it converts the original and meaningful content to incomprehensible one. Although few RDH techniques in encrypted images have been published yet, there are some promising applications if RDH can be applied to encrypted images.

Key words: Reversible Data Hiding, Image Encryption, Privacy Protection

I. Introduction

Reversible data hiding (RDH) in images is a technique, by which the original cover can be losslessly recovered by which the original cover can be lossless recovered after the embedded message is extracted. This important techniques widely used in medical imagery, military imagery and law forensics, where no distortion of the original cover is allowed. Since first introduced, RDH has attracted consider a bleresearch interest. In theoretical aspect, stablished arate-distortion model for RDH, through which they proved the rate-distortion bounds of RDH for memory less covers and proposed a recursive code construction which, however, does not approach the bound. Improved the recursive code construction for binary covers and proved that this construction can achieve the rate-distortion bound as long as the compression algorithm reaches entropy, which establishes methods mentioned above rely on spatial correlation of original image to extract data. That is, the encrypted image should be decrypted first before data extraction.

To separate the data extraction from image decryption,emptied out space for data embedding following the idea of compressing encrypted images. Compression of encrypted data can be formulated as source coding with side information at the decoder, 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 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 images. All the three methods try to vacate room from the encrypted images directly. However, since the entropy of encrypted images has been maximized, these techniques can only achieve small payloads or generate marked image with poor quality for large payload and all of them are subject to some error rates on data extraction and/or image restoration. Although the methods in 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 images, for which we do not “vacate room after encryption” as done in , but “reserve room before encryption”. In the proposed method, we first empty out room by embedding LSBs of some pixels into other pixels with a traditional RDH method and then encrypt the image, so the positions of these LSBs in the encrypted image can be used to embed data. Not only does the proposed method separate data extraction from image decryption but also achieves excellent performance in two different prospects:

1) Real reversibility is realized, that is, data extraction and image recovery are free of any error.
2) For given embedding rates, the PSNRs of decrypted image containing the embedded data are significantly improved.

II. Existing System

In the Existing System, since lossless vacating room from the encrypted images is relatively difficult and sometimes inefficient, why are we still so obsessed to and novel RDH techniques working directly for Encrypted Images. The method in 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 images.

A. Disadvantages:

1) Low error rate.
2) Data extraction and Image resolution problem.

III. Proposed System

Since losslessly vacating room from the encrypted images is relatively difficult and sometimes inefficient, why are we still so obsessed to find novel RDH techniques working directly for encrypted images? If we reverse the order of encryption and vacating room, i.e., reserving room prior to image encryption at content owner side, the RDH tasks in encrypted images would be more natural and much easier which leads us to the novel framework, “reserving room before encryption (RRBE)”. As shown in Fig. the content owner first reserves enough space on original image and then converts the image into its encrypted version with the encryption key. Now, the data embed ding process in encrypted images is inherently reversible for the data hider only needs to accommodate data into the spare space previous emptied out. The data extraction and image recovery are identical to that of Framework VRAE. Obviously, standard RDH algorithms are the ideal operator for reserving room before encryption and can be easily applied to Framework RRBE to achieve better performance compared with techniques from Framework VRAE. This is because in this new framework, we follow the customary idea that first losslessly compresses the redundant image content (e.g., using excellent RDH techniques) and then encrypts it with respect to protecting privacy.

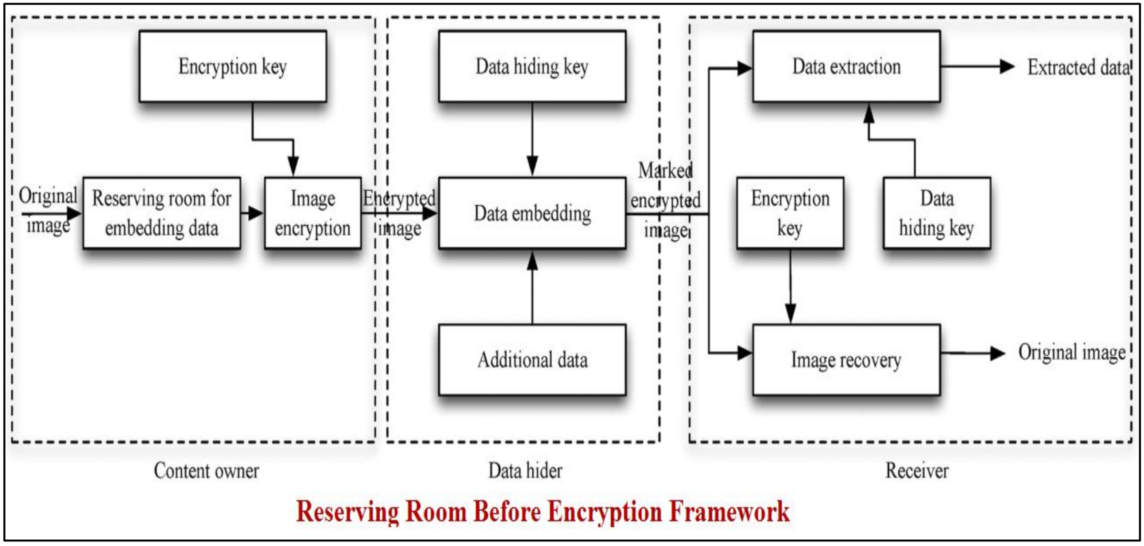

Fig. 1: System Architecture

A. *Advantages of Proposed System:*

1) Not only does the proposed method separate data extraction from image decryption but also achieves excellent performance in two different prospects.
2) Real reversibility is realized, that is, data extraction and image recovery are free of any error.
3) For given embedding rates, the PSNRs of decrypted image containing the embedded data are significantly improved; and for the acceptable PSNR, the range of embedding rates is greatly enlarged.

IV. ALGORITHM

A. *RC4 Algorithm:*

RC4 is a stream cipher, symmetric key algorithm. The same algorithm is used for both encryption and decryption as the data stream is simply XORed with the generated key sequence. The key stream is completely independent of the plaintext used. It uses a variable length key from 1 to 256 bit to initialize a 256-bit state table. The state table is used for subsequent generation of pseudo-random bits and then to generate a pseudo-random stream which is XORed with the plaintext to give the cipher text.

RC4 is a stream cipher designed in 1987 by Ron Rivest for RSA Security. It is a variable keysize stream cipher with byte-oriented operations. The algorithm is based on the use of a random permutation. Analysis shows that the period of the cipher is overwhelmingly likely to be greater than 10100 [ROBS95]. Eight to sixteen machine operations are required per output byte, and the cipher can be expected to run very quickly in software. RC4 was kept as a trade secret by RSA Security. In September 1994, the RC4 algorithm was anonymously posted on the Internet on the Cypherpunks anonymous remailers list.

The RC4 algorithm is remarkably simply and quite easy to explain. A variable-length key
of from 1 to 256 bytes (8 to 2048 bits) is used to initialize a 256-byte state vector S, with

Elements S[0], S[1], …, S[255]. At all times, S contains a permutation of all 8-bit numbers from 0 through 255. For encryption and decryption, a byte k (see Figure 1) is generated from S by selecting one of the 255 entries in a systematic fashion. As each value of k is generated, the entries in S are once again permuted.

B. *Initialization of S:*

To begin, the entries of S are set equal to the values from 0 through 255 in ascending order; thatis; S[0] = 0, S[1] = 1, …, S[255] = 255. A temporary vector, T, is also created. If the length of the key K is 256 bytes, then K is transferred to T. Otherwise, for a key of length keylen bytes, the first keylen elements of T are copied from K and then K is repeated as many times as necessary to fill out T. These preliminary operations can be summarized as follows:

```
/* Initialization */
for i = 0 to 255 do
S[i] = i;
T[i] = K[i mod keylen];
```

Next we use T to produce the initial permutation of S. This involves starting with S[0] and going through to S[255], and, for each S[i], swapping S[i] with another byte in S according to a scheme dictated by T[i]:

```
/* Initial Permutation of S */:
j = 0;
for i = 0 to 255 do
j = (j + S[i] + T[i]) mod 256;
Swap (S[i], S[j]);
```

Because the only operation on S is a swap, the only effect is a permutation. S still contains all the numbers from 0 through 255.

C. *Stream Generation:*

Once the S vector is initialized, the input key is no longer used. Stream generation involves

Starting with S[0] and going through to S[255], and, for each S[i], swapping S[i] with another

Byte in S according to a scheme dictated by the current configuration of S. After S[255] is

Reached, the process continues, starting over again at S [0]:

```
/* Stream Generation */:
i, j = 0;
-6-
while (true)
i = (i + 1) mod 256;
j = (j + S[i]) mod 256;
Swap (S[i], S[j]);
t = (S[i] + S[j]) mod 256;
k = S[t];
```

To encrypt, XOR the value *k* with the next byte of plaintext. To decrypt, XOR the value *k*
With the next byte of cipher text.

D. Strength of RC4:

A number of papers have been published analyzing methods of attacking RC4 [e.g., [KNUD98], [MIST98], [FLUH00], [MANT01]). None of these approaches is practical against RC4 with a reasonable key length, such as 128 bits. A more serious problem is reported in [FLUH01]. The authors demonstrate that the WEP protocol, intended to provide confidentiality on 802.11 wireless LAN networks, is vulnerable to a particular attach approach. In essence, the problem is not with RC4 itself but the way in which keys are generated for use as input to RC4. This particular problem does not appear to be applicable to other applications using RC4 and can be remedied in WEP by changing the way in which keys are generated. This problem points out the difficulty in designing a secure system that involves both cryptographic functions and protocols that make use of them.

V. MATHEMATICAL MODEL OF OUR PROJECT

Let M be the Mathematical Model which Consists Of User set, Server And Admin
M={U,S,D};
U = {U1,U2,-----,Un} ---Set of users
D - Database
A- Admin

A. Mapping:

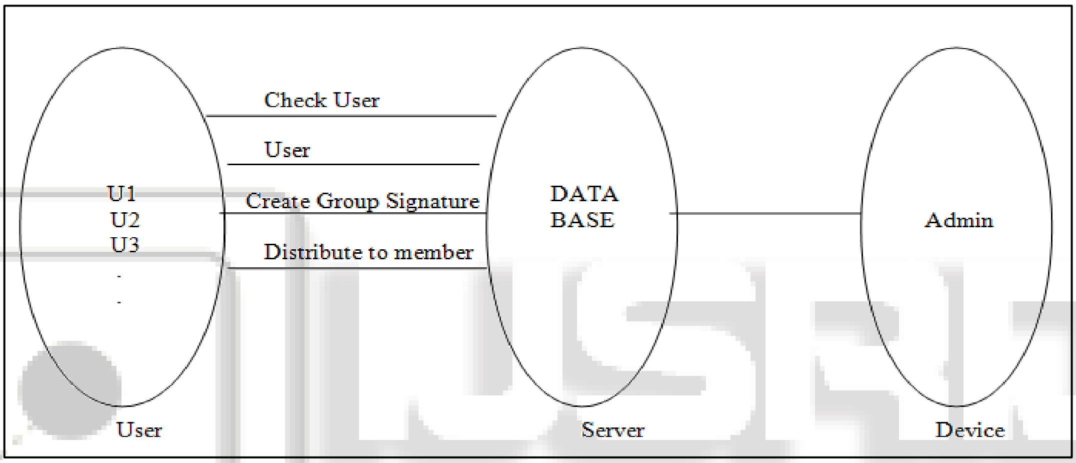

Fig. 2: Mathematical Model which Consists Of User set, Server and Admin

Let U1,….. Un be the set of user who will first log in and will apply for group signature And D- be the Database If user is authorized then database will store and notified to Admin. A-be the Admin set when Admin will receive the watermark, he will distribute group signature

VI. GRAPH

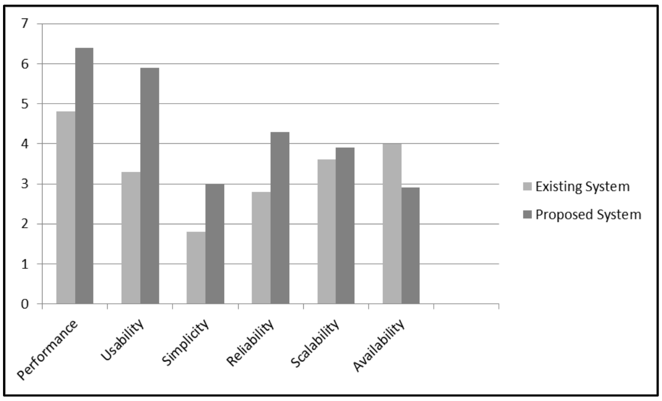

Fig. 3: Performance of System

A. Performance:

Building high performance software systems requires an understanding of the behaviour of systems and what makes them fast or slow. Depending on the context, high computer performance may involve short response time for a given piece of work, high throughput, low utilization of computer resources, high bandwidth.

B. Usability:

Usability is the ease of use and learnability of a human-made object. Usability includes methods of measuring needs analysis and the study of the principles behind an object's perceived efficiency or elegance. Usability also studies the elegance and clarity with which the interaction with a computer program is designed. There are varieties of usability evaluation methods. Certain methods use data from users, while others rely on usability experts.

In the existing system, the rating given is 3.2 units, the reason behind the same is that the ease of use and learnability of a human-made object in the existing system is low as compared to the proposed system. The different attributes of usability are efficiency, memorability, errors and satisfaction. So, the existing system fails in these attributes, so it lags behind the proposed system.

In the proposed system, the rating given is 5.8 units, the reason for the same is that the proposed system, boost the usability of system by improving learnability of system, increasing efficiency, more memorability. It also reduces the occurrences of errors to the least numbers, and gives much more satisfaction.

C. Simplicity:

Simplicity is the state or quality of being simple. Something which is easy to understand or explain is simple, in contrast to something complicated. The 'keep it simple, stupid' principle states that most system work best if they are kept simple rather than made complex; therefore simplicity should be a key goal in design and unnecessary complexity should be avoided.

In the existing system, the rating given in above graph for simplicity is 1.8, because of the complexities associated with the software system. It was not a best experience for a user to handle the software system as it was somewhat complex. In the proposed system, the rating given for simplicity is 3 units, because as compared to the existing system, the proposed system is somewhat simple in use for user. As there are no much more complexities are associated with the proposed system, so it will be advantage to use the proposed system in case of simplicity.

D. Reliability:

Reliability refers to the ability of a system or component to perform its required functions under the stated conditions for a specified period of time.

In the existing system, the system has rating of 2.8 units, because the system is not that much reliable as compared to the proposed system. The system gets lot much time to respond a request when it gets lot much load of data and processing. In the proposed system, rating given is 4.2 units, because the system has reliability somewhat better than existing system. In the proposed system, reliability plays a vital role to make it better product as compared to the existing stem.

E. Scalability:

Scalability refers to the ability of a system, network, or process to handle a growing amount of work in a capable manner or its ability to be enlarged to accommodate that growth. For example, it can refer to the capability of a system to increase its total output under an increased load when resources are added. A system, whose performance improves after adding hardware, proportionally to the capacity added, is said to be a scalable system. Scalability can be measured in various dimensions, such as functional scalability, load scalability, generation scalability.

F. Availability:

Availability of a system refers to the characteristic of a resource that is committable, operable, or usable upon demand to perform its designed or required function.

VII. Result

Pseudo random sequence consists of random bits generated using the encryption key. In our system, RC-4 algorithm is used to create the pseudo-random sequence using the 128-bit encryption key. The additional data inserted to encrypted image using the parameters. With an encrypted image containing additional data, the receiver may extract the additional data using only the data-hiding key, or obtain an image similar to the original one using only the encryption key. When using both of the encryption and data-hiding keys, the embedded additional data can be successfully extracted and the original image can be perfectly recovered by exploiting the spatial correlation in natural image. Compared with the other algorithms, the proposed system demonstrated successful accuracy in recovering the original images.In the future, a comprehensive combination of image encryption and data hiding compatible with loss compression deserves further investigation.

VIII. Conclusion

Main objective of project is to provide the security while sending any important or secure data by encrypting images various online applications using the images. Project provides security to data which is encrypted in that using reversible data hiding encrypted images.

IX. Acknowledgement

The development of the system "Reversible Data Hiding in Encrypted Images Using RC4 Algorithm" has given us immense pleasure and knowledge. We are sincerely thankful to the project guide Prof. Paresh D. Sonawane who has cooperated with us at different stages during the preparation of this system. Our sincere thanks to the staff of Computer Engineering without whose help it would not have been possible for us to complete this report. This work is virtually the result of inspiration given by them. We would also like to thank all the library and the non-teaching staff for their help and last but not least we would like to thank all out friends for their constant help and support.

References

[1] T.Kalkerand, F.M.Willems, "Capacity bounds and code constructions for reversible data-hiding", in Proc.14th Int. Conf. Digital Signal Pro- cessing (DSP2002), 2002, pp. 71–76.

[2] W. Zhang, B. Chen, and N. Yu, "Capacity-approaching codes for reversible data hiding," in Proc 13th Information Hiding (IH'2011), LNCS 6958, 2011, pp. 255–269, Springer-Verlag.

[3] W. Zhang, B. Chen, and N. Yu, "Improving various reversible data hiding schemes via optimal codes for binary covers," IEEE Trans. Image Process., vol. 21, no. 6, pp. 2991–3003, Jun. 2012.

[4] X. L. Li, B. Yang, and T. Y.Zeng, "Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection," IEEE Trans. Image Process. vol. 20, no. 12, pp. 3524–3533, Dec. 2011.

[5] Kede Ma, Weiming Zhang, Xianfeng Zhao , Nenghai Yu, and Fenghua Li. "Reversible data hiding in encrypted images by reserving room before encryption". IEEE transactions on information forensics and security, vol. 8, no. 3, march 2013.

[6] V. Suresh, C. Saraswathy, "Separable reversible data hiding using rc4 algorithm". Department of Electronics and Communication Engineering, K.S.Rangasamy College of Technology, India IEEE Trans. Inform. Forensics Security, vol. 6, no. 1, pp. 53–58, Feb. 2011.

[7] Parag Kadam, Mangesh Nawale, "Seperable reversible encrypted data hiding in encrypted

images using AES algorithm and loss technique." vol. 7, no. 2, pp. 826-32,April 2012.

[8] 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.