Impact Factor (SJIF): 3.632

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 3, Issue 4, April-2016

Separable Reversible Data Hiding with RC4 Algorithm

Prof. R. D. Shelke[1], Nikhil Umale[2], Ravindra Chavare[3] Sushant Bandekar[4]

Department of Electronics & Telecommunication, Shivajirao S. Jondhale College of Engineering, University of Mumbai

Abstract — this paper proposes a unique technique for separable reversible information hiding in encrypted pictures. Within first phase, a content owner encrypts the initial uncompressed image using a cryptographic key that uses RC4 cryptographic algorithm. Then, an information-hider may compress the smallest amount significant bits of the encrypted image using a data-hiding key using LSB technique accommodate small amount of data. With an encrypted image containing extra information, if a receiver has the data-hiding key, he will extract the extra information although it doesn't recognize the image content. If the receiver has the cryptography key, it can decode the received information to get a picture almost like the initial one, however cannot extract the extra information. If the receiver has both data-hiding key as well as cryptography key, it can extract information and recover the initial content with none error by exploiting the spatial correlation in natural image once the quantity of additional information isn't overlarge.

Keywords- Image encryption; image recovery; reversible data hiding; discrete cosine transform;Difference expansion

I. INTRODUCTION

In recent years, image compression has attracted considerable research area. The traditional method includes the way of securely and efficiently transmitting redundant data is to compress the data to reduce the redundancy and then to encrypt the compressed data and to masks it's meaning. At the receiver side, the decryption and decompression operations are orderly performed to recover the original data. In a recent scenario, a sender needs to transmit some data to a receiver and hopes to keeps the information confidential from network operator who provides the channel resource for the transmission. Several techniques for compressing and decompressing encrypted data have been developed.Data hiding is to conceal the existence of secret data. A separable reversible data hiding method can extract the cover image without any distortion from the stego-image after the hidden data have been extracted. Data hiding is a form of steganography, embeds data into digital media for the purpose of identification, annotation, and copyright. Several constraints affect this process: the quantity of data to be hidden, the need for invariance of these data under conditions where a "host" signal is subject to distortions. The paper is further organized into four sections.

I. Overview of RC4: - discusses RC4 encryption algorithm.
II. Literature survey: - discusses previous studies related encryption, decryption, data hiding, reversible data hiding etc.
III. Implementation Overview: - discusses the proposed system.
IV. Conclusion: - concludes the paper.

II. OVERVIEW OF RC4

The RC4 algorithm generates a pseudo-random key-stream that is then used to generate the cipher-text (by XOR it with the plaintext). It is called pseudo-random because it generates a sequence of numbers that only approximates the properties of random numbers. The key-stream is generated from a variable length key using an internal state composed of the following elements.

- A 256 bytes array (denoted S) containing a permutation of these 256 bytes.
- Two indexes p and q, used to point elements in the S array (only 8 bits are necessary for each index since the array only have 256 elements).

III. LITERATURE SURVEY

As the image compression is the wide area of research. There are several types of techniques have been proposed in this domain.[1] proposes Implementation of Modified RC4 Stream Cipher Using FPGA explains efficient hardware implementation of RC4 algorithm. [2] Proposes Analysis of JPEG Images :- Breaking the F5 Algorithm that gives overview of F5 data embedding algorithm. [3] Proposes Buyer-Seller watermarking protocol video fingerprinting and encryption principles for digital rights management in which invisible watermarking in which the seller does not get to know the exact watermarked copy that the buyer receives. [4] proposes universal image quality index to assess perpetual image quality traditionally attempted to quantify the visibility of errors b/w a distorted image and a reference image using a variety of known properties of the human visual system.[5] proposed Lossless Information Hiding Scheme Based on Neighboring Correlation was projected which hides secret information into gray-level images according to the correlation between neighboring pixels.[6] proposes the fundamentals of data hiding security and their application to

spread application to spread-spectrum analysis is discussed. [7] Explains about hiding scheme that hides secret information into gray-level images according to the correlation between neighboring pixels. [8] spectrum analysis in which the fundamentals of Fundamentals of data hiding security and their proposes reversible data-embedding scheme using differences between original and predicted pixel values that includes reversible data embedding scheme to embed secret information in original images. [9] presented secure spread spectrum watermarking for multimedia in which a method for digital watermarking is proposed. [10] represents efficient compression of encrypted grayscale images in which a compression scheme is mentioned which compresses an encrypted image progressively in resolution. However, the above mentioned techniques produces insufficient results and used for used for obtaining different results. Our proposed technique demonstrated successful accuracy in recovering the original image.

III. IMPLEMENTATION DETAILS

The proposed system will consist of three major modules:

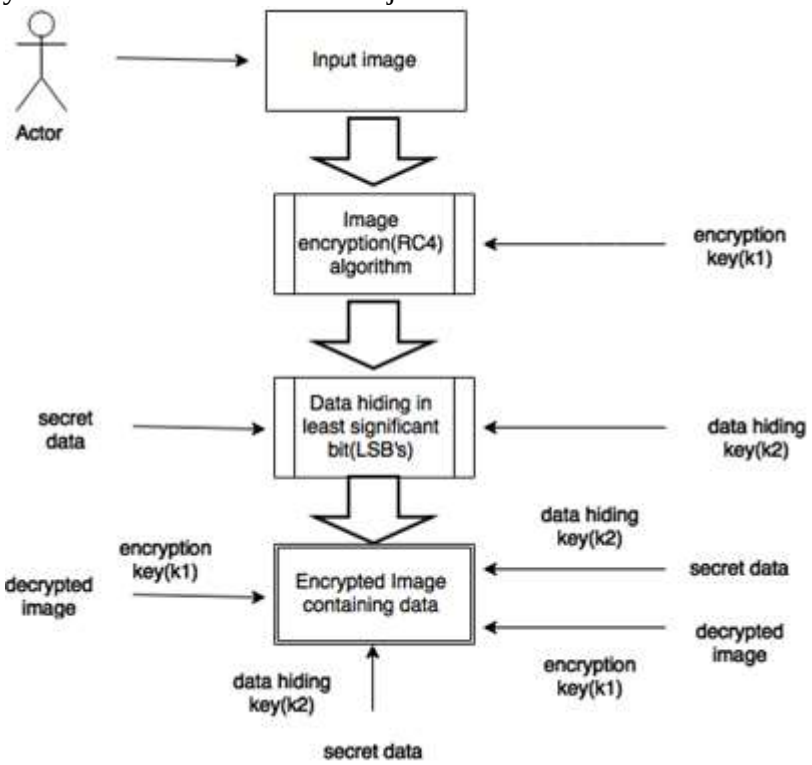

Figure 1. Block diagram of proposed system

Figure 2 shows the architectural design of the proposed system. Initially, the image Undergo encryption phase. Encryption is performed by RC4 secret key algorithm, encryption key (k1) is taken as input. After image encryption secret data is embedded into encrypted image proving data hiding key (k2) as input. On the receiver if receiver has data hiding key (k2) then receiver can extract secret data, though receiver unable to decrypt image. If receiver has encryption key (k1), receiver can decrypt image though the image contain small amount of secret data. If receiver has both keys can extract secret data as well as decrypt image without any error.

- **Image encryption:**

The steps for RC4 encryption algorithm are:

1. Get the Original image array and key.
2. Create two string arrays.
3. Initialize one array with numbers from 0 to 255.
4. Fill the other array with key.
5. Randomize the first array depending on the array of the key.
6. Randomize the first array within itself to generate the final key stream.
7. XOR the final key stream with original image array to give encrypted image.

- **Data Hiding:**

The steps for LSB data embedding as per [25] are:

1. Data hider first selects encrypted image of size N = N1×N2 and data hiding key.
2. Some parameters (M, L and S) for data hiding are embedded in small number of encrypted pixel Np.
3. Remaining (N-Np) encrypted pixels are pseudo-randomly permuted to generate matrix Q It is divided into number of groups of L pixels. Permutation is dependent on data hiding key.
4. For each group, select M least significant bits of L pixels. let us denote them as B (k, 1), B (k; 2), _ _ _, B (k,ML) where k is group index with in [1, (N-Np)/M] and M is a positive integer less than 3.
5. The data hider also generates a matrix G of size (ML-S) ×S:

$$G = \left[I_{ML-S} \quad Q \right]$$

Where, left part is an identity matrix of size (ML- S) × (ML- S) the right part Q is (ML-S) ×S is a pseudo-random binary matrix generated in step 3.

6. For each group of L pixel calculate.

$$\begin{bmatrix} B'(k,1)) \\ B'(k,2)) \\ . \\ . \\ . \\ B'(k,ML-S) \end{bmatrix} = G \bullet \begin{bmatrix} B(k,1)) \\ B(k,2)) \\ . \\ . \\ . \\ B(k,ML) \end{bmatrix}$$

Where **.** represents arithmetic modulo-2 [B(k, 1),B(k, 2), ,B(k, ML)] are compressed to create sparse space to accommodate some additional data.

7. After above step, the (8-M) most significant bits (MSB) of encrypted pixels are kept unchanged.
8. S bits are embedded into each pixel group; the total bits can be embedded in all groups. Clearly, the embedding rate R, a ratio between the data amount of net payload and the total number of cover pixels is

$$R = \frac{((N - N_P).S/L)}{N} \approx \frac{S}{L}$$

- **Data Extraction/ Image Recovery**

Data extraction and image recovery is performed at the receiver side. As for the decryption, it is as simple as the encryption we only have to do the opposite: XOR the cipher text with the key stream. The RC4 algorithm encrypts an image containing additional data, a receiver may first decrypt it according to the encryption key, and then extract the embedded data and recover the original image according to the data-hiding key. In this technique data extraction and image recovery are independent of each other.

IV. CONCLUSION

In this paper, we have proposed a unique technique called separable reversible data hiding using RC4 algorithm. Initially, user sends an image for the encryption using RC4 algorithm. With an encrypted image containing additional information, the receiver may extract knowledge using only the data-hiding key or acquire an image similar to the rest one using only the encryption key. Once the receiver has each of the keys, can extract the additional information as well as recovered image. Sender can encrypt original image using RC4 algorithm while data hider can embed data by using LSB data embedding technique. This paper also proposes lossy compression.

Acknowledgment

We are thankful to our guide Prof. R. D. Shelke for his guidance and encouragement in this work. His expert suggestions and scholarly feedback had greatly enhanced the effectiveness of this work. We are also thankful to Prof. S. A. Lonkar, Head of Department, Electronics Telecommunication, S.S.J.C.E Dombivli. .We would also like to express my appreciation and thanks to Dr. J. W. Bakal, Principal, S.S.J.C.E Dombivli. We would also like to express my appreciation and thanks to all my colleagues and family members who knowingly or unknowingly have assisted and encouraged us throughout our journey.

REFERENCES

[1] Jaya Dofe & Manish Patil, Hardware Implementation of Modified RC4 Stream Cipher Using FPGA.
[2] Sunny Binghamton : Analysis of JPEG Images :- Breaking the F5 Algorithm. "Department of Electrical and Computer Engineering NY 13902-6000, USA"
[3] Nasir Memon &Ping Wah Wong, A Buyer-Seller Watermarking Protocol Video fingerprinting and encryption principles for digital rights management.
[4] Z. Wang, A universal image quality index
[5] M. U. Celik, G. Sharma , Lossless Information Hiding Scheme Based on Neighboring Correlation
[6] P. Comesan,L. Perez-Frieri, Fundamentals of data hiding security and their application to spread-spectrum analysis.
[7] M. U. Celik, G. Sharma, Lossless Information Hiding Scheme Based on Neighboring Correlation.
[8] E. Corchado, M.A. Pellicer, M.L. Borrajo, A MLHL based method to an agent-based architecture, International Journal of Computer Mathematics 86
(2009) 1760–1768.
[9] C. Chang , Reversible data-embedding scheme using differences between original and predicted pixel values.
[10] I.J Cox, Secured spread spectrum watermarking for multimedia.
[11] W. Liu, W. Zeng , Efficient Compression of Encrypted Grayscale Images.
[12] X. Zhang, "Lossy compression and iterative reconstruction for encrypted image," IEEE Trans. Inform. Forensics Security, vol. 6,no. 1, pp. 53–58, Feb. 2011.
[13] W. Liu, W. Zeng, L. Dong, and Q. Yao, "Efficient compression of encrypted grayscale images," IEEE Trans. Image Process., vol. 19, no. 4, pp. 1097–1102, Apr. 2010.
[14] S. Lian, Z. Liu, Z. Ren, and H. Wang, "Commutative encryption and watermarking in video compression," IEEE Trans. Circuits Syst. VideoTechnol., vol. 17, no. 6, pp. 774–778, Jun. 2007.
[15] M. Cancellaro, F. Battisti, M. Carli, G. Boato, F. G. B. Natale, and A Neri, "A commutative digital image watermarking and encryptionmethod in the tree structured Haar transform domain," *Signal Processing*.
[16] *Image Commun.*, vol. 26, no. 1, pp. 1–12, 2011.Z. Wang and A. C. Bovik, "A universal image quality index," *IEEESignal Process. Lett.*, vol. 9, no. 1, pp. 81–84, Jan. 2002.
[17] Andreas Westfield, A high steganographic algorithm high capacity despite better staganalysis.
[18] Steganography of high embedding efficiency using an extended matrix encoding algorithm.
[19] Yong soo choi,Hyoun joong kim, Improving the modified matrix encoding on steganography method. 2009 Fifth International Conference on Information Assurance and Security.
[20] Gaurav Prasad and Sujay Narayana, A novel approach for concealed data
sharing and data embedding for secured communication.
[21] Sunila godara,Megha Ranolia, Vanita Rawal ,Comparitive study of image steganography technique.
[22] Hedieh Sajedi, RABS: Rule based adaptive batch steganography,
[23] Chin-yung Lin, Watermarking and Digital signature technique for multimedia authentication and copyright protection.
[24] Sunny Binghamton : Analysis of JPEG Images :- Breaking the F5 Algorithm. "Department of Electrical and Computer Engineering NY 13902-6000, USA"
[25] Xinpeng Zhang, Separable Reversible Data Hiding in Encrypted Image IEEE Transaction on Information Forensic and Security Vol 7 No.2 April 2012.