International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal
ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 2

Image Realization Steganography by Secure Key Transmission

S. Angelin Nivedita
Department of CSE, Mailam Engineering College, Villupuram, Tamil Nadu, India

Dr. T. Priyaradhikadevi
Professor and Head, CSE, Mailam Engineering College, Villupuram, Tamil Nadu, India

ABSTRACT

This work proposes a novel scheme for separable reversible data hiding in encrypted images. In the first phase, a content owner encrypts the original uncompressed image using an encryption key. Then, a data-hider may compress the least significant bits of the encrypted image using a data-hiding key to create a sparse space to accommodate some additional data. With an encrypted image containing additional data, if a receiver has the data-hiding key, can extract the additional data though the image content is not known. If the receiver has the encryption key, then can decrypt the received data to obtain an image similar to the original one, but cannot extract the additional data. If the receiver has both the data-hiding key and the encryption key, can extract the additional data and recover the original content without any error by exploiting the spatial correlation in natural image when the amount of additional data is not too large.

Keywords: *Image Steganography, Encryption, Decryption, Extraction key, Segmentation*

I. INTRODUCTION

Data mining, *the extraction of hidden predictive information from large databases*, is a powerful new technology with great potential to help companies focus on the most important information in their data warehouses. Data mining tools predict future trends and behaviors, allowing businesses to make proactive, knowledge-driven decisions. The automated, prospective analyses offered by data mining move beyond the analyses of past events provided by retrospective tools typical of decision support systems. Data mining tools can answer business questions that traditionally were too time consuming to resolve. They scour databases for hidden patterns, finding predictive information that experts may miss because it lies outside their expectations. Data mining techniques can be implemented rapidly on existing software and hardware platforms to enhance the value of existing information resources, and can be integrated with it.

Web structure mining, one of three categories of web mining for data, is a tool used to identify the relationship between Web pages linked by information or direct link connection. This structure data is discoverable by the provision of web structure schema through database techniques for Web pages. This connection allows a search engine to pull data relating to a search query directly to the linking Web page from the Web site the content rests upon. This completion takes place through use of spiders scanning the Web sites, retrieving the home page, then, linking the information through reference links to bring forth the specific page containing the desired information.

With the rapid advancement in network technology especially Internet, it has become possible to transmit any type of digital data across networks. This has raised concerns for the security of the transmitted data as access to it has become easier by interception of communication media. Hence digital data security is becoming an imperative and critical issue in data storage and transmission to prevent it from attacks.

Images are widely used in several processes. Therefore, the protection of image data from unauthorized access is important. In this paper, our research focuses on reversible data hiding in encrypted images.

Encryption and steganography are means to accomplish data security. Encryption refers to the algorithmic schemes that encode the original message referred to as plain text using a key into non-readable form, a coded message known as cipher text so that it is computationally infeasible to be interpreted by any eavesdropper. The receiver of the cipher text uses a key to retrieve back the message in original plain text form.

In our scheme we propose reversible data hiding scheme in encrypted images. The following are the major contribution of our scheme:

1) In our scheme we provide, secure key transmission for securely sending confidential information.
2) By integrating algorithms / techniques we can protect valuable data or image from undesirable readers
3) Faster recovery and processing of data. This would significantly decrease the processing time of load balancer.
4) Descrambling is not possible because the user is the only party apart from the provider to possess the key for descrambling,
5) The Peak Signal Noise Ratio of decrypted image containing the embedded data are significantly improved; and for the acceptable the range of embedding rates is greatly enlarged.

II. LITERATURE SURVEY

Shi Liuy [1] Optical information hiding techniques have received significant attention recently, due to their considerable advantages, such as inherent capabilities for parallel ultra-fast processing, and the possibility of their applications to biometrics, optical security and product authenticity verification a novel scheme for optical information hiding (encryption) of two-dimensional images by combining image scrambling techniques in fractional Fourier domains. The image is initially random shifted using the jigsaw trans- form algorithm, and then a pixel scrambling technique based on the Arnold transform (ART) is applied. Then, the scrambled image is iteratively encrypted in the fractional. Fourier domains using randomly chosen fractional orders. The parameters of the architecture, including the jigsaw permutations indices, Arnold frequencies, and fractional Fourier orders, form a huge key space enhancing the security level of the proposed encryption system. Optical implementations are discussed and numerical simulation results are presented to demonstrate the exibility and robustness. The fractional Fourier transform (FRT) and its optical implementations have been studied for several years.

Qin Zheng Liu Bo [2] Conventional scrambling methods based on permuting pixels coordinates can be used to construct robust water markings which can endure erasing, cropping and compressing attacks. But most of these methods are used to scramble equilateral image, for the non equilateral image where its width not equal to its height, it is usually expanded into equilateral image or partitioned into several equilateral images, which increases the cost for extra space or operating complexity. Although there are some methods which can scramble non equilateral image, these methods need to construct coordinate shifting path first and the cost to build coordinate shifting path is usually expensive. To address these problems, in this study, we propose a new scrambling algorithm based on random shuffling strategy, which can scramble non equilateral image and has a low cost to build coordinate shifting path. The proposed algorithm has a good one time scrambling performance. It can be used to scramble or recover image in real time and can also resist the JPEG compression attacks. Experiments show the proposed scrambling method validity in scrambling or recovering non equilateral image and robustness in enduring erasing, cropping and JPEG compressing attacks. Since the user defined sequence which can be from 10 to 100 values long positive integers in the range of 1 to 200, statistically, the probability of estimating such a sequence will be (1/200)100 = 5x10-300. Hence we can conclude that estimating such a sequence to unscramble the image will be practically impossible.

Prashan Premaratne [3] Digital images are increasingly sent over networks as documents, commercial items or law enforcement material. Due to the heightened activities of hackers all over the world, these images can easily end up in the hands of unscrupulous third parties who might profit/extort or modify them without the knowledge of the legitimate

receiver. Secure image communication is becoming increasingly important due to theft and manipulation of its content. Law enforcement agents may find it increasingly difficult to stay afloat above the ill intentions of hackers. We have been able to develop an image scrambling algorithm that is very simple to implement but almost impossible to breach with a probability less than 5x10-300. This is possible due to the fact that a user may purchase or acquire rights for an intended image by specifying a 'key' that can form a sequence of numbers 10 to 100 in length. The content provider uses this sequence as a base in developing another key sequence to scramble the image and transmit it to the user through regular channels such as an email attachment. Since the user is the only party apart from the provider to possess the key for descrambling, any third party will not be able to descramble it successfully.

P. Radhadevi [4] Security in transmission of digital images has its importance in today's image communications, due to the increasing use of images in industrial process, it is essential to protect the confidential image data from unauthorized access, Image security has become a critical issue. The difficulties in ensuring individuals privacy become increasingly challenging. Various methods have been investigated and developed to protect data and personal privacy. Encryption is probably the most obvious one. In order to protect valuable information from undesirable readers, image encryption is essential. This paper presents an application of AES (Advanced Encryption Standard) operations in image encryption and decryption. The encrypted cipher images always display the uniformly distributed RGB pixels. Encryption involves applying special mathematical algorithms and keys to transform digital data into cipher code before they are transmitted and decryption involves the application of mathematical algorithms and keys to get back the original data from cipher code, scientific community have seen strong interest in image transmission. However, illegal data or image access has become more easy and prevalent in wireless and general communication networks. Information privacy becomes a challenging issue. In order to protect valuable data or image from undesirable readers, data or image encryption / decryption is essential, furthermore. As such in this paper, a scheme based on encryption has been proposed for secure image transmission over channels.

III. PROPOSED SYSTEM

In proposed method can achieve real reversibility, that is, data extraction and image recovery are free of any error. 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). The system also proposed hash algorithm and stegnography techniques to improving the security and complexity. A hash function is any function that can be used to map data of arbitrary size to data of fixed size. The values returned by a hash function are called hash values, hash codes, digests, or simply hashes. One use is a data structure called a hash table, widely used in computer software for rapid data lookup. A hash function must be able to process an arbitrary-length message into a fixed-length output. Steganography is a useful technique for hiding data behind the carrier file such as image, audio, video etc. and that data securely transfer from sender to receiver

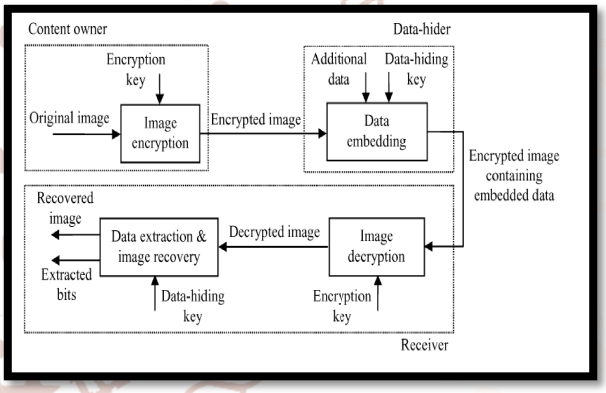

Fig.1 system architecture

AUTHENTICATION SENDER AND RECEIVER:

The sender send a data to the authorized person by sending an image with secrete key to the receiver confidentially for sending and receiving a data.

IMAGE ENCRYPTION

In this module, to construct the encrypted image, the first stage can be divided into three steps:

a) Image partition,
b) Self reversible embedding followed by image encryption.

At the beginning, image partition step divides original image into two parts and then, the LSBs of are

reversibly embedded into with a standard RDH algorithm so that LSBs of can be used for accommodating messages; at last, encrypt the rearranged image to generate its final version. The data before encryption is a standard RDH technique.

SIGNATURE GENERATION

The first phase is a choice of algorithm parameters which may be shared between different users of the system, while the second phase computes public and private keys for a single user. The goal of self-reversible embedding is to embed the LSB-planes of into by employing traditional RDH algorithms. We simplify the method in to demonstrate the process of self-embedding. In this module, a content owner encrypts the original image using a standard cipher with an encryption key. After producing the encrypted image, the content owner hands over it to a data hider (e.g., a database manager) 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.

IMAGE RECOVERY

In this module, Extracting Data from Encrypted Images to manage and update personal information of images which are encrypted for protecting clients' privacy, an inferior database manager may only get access to the data hiding key and have to manipulate data in encrypted domain. When the database manager gets the data hiding key, he can decrypt and extract the additional data by directly reading the decrypted version. When requesting for updating information of encrypted images, the database manager, then, updates information through LSB replacement and encrypts up dated information according to the data hiding key all over again. As the whole process is entirely operated on encrypted domain, it avoids the leakage of original content.

ADVANCED ENCRYPTION STANDARD (AES)

The Advanced Encryption Standard (AES), also known as Rijndael (its original name), is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001. AES is a subset of the Rijndael cipher developed by two Belgian cryptographers, JoanDaemen and Rijmen, who submitted a proposal to NIST during the AES selection process. Rijndael is a family of ciphers with different key and block sizes.

AES operates on a 4 × 4 column-major order matrix of bytes, termed the state, although some versions of Rijndael have a larger block size and have additional columns in the state. Most AES calculations are done in a special finite field. AES consists of several rounds of several processing steps that include substitution, transposition and mixing of the input plaintext and transform it into the final output of ciphertext.

AES : Pseudocode

```
Cipher(byte in[16], byte out[16], key_array round_key[Nr+1])
begin
byte state[16];
state = in;
AddRoundKey(state, round_key[0]);
for i = 1 to Nr-1 stepsize 1 do
SubBytes(state);
ShiftRows(state);
MixColumns(state);
AddRoundKey(state, round_key[i]);
end for
SubBytes(state);
ShiftRows(state);
AddRoundKey(state, round_key[Nr]);
End
```

REVERSIBLE DATA HIDING

Reversible Data Hiding in encrypted images attracts more and more researchers' attention. It is different from all encryption-based frameworks, in which the ciphertexts may attract the notation of the curious cloud, RIT-based framework allows the user to transform the content of original image into the content of another target image with the same size. The transformed image, that looks like the target image, is used as the "encrypted image," and is outsourced to the cloud. Therefore, the cloud server can easily embed data into the "encrypted image" by any RDH methods for plaintext images. And thus a client-free scheme for RDH-EI can be realized, that is, the data-embedding process executed by the cloud server is irrelevant with the processes of both encryption and decryption. Two RDH methods, including traditional RDH scheme and unified embedding and scrambling scheme, are adopted to embed watermark in the encrypted image, which can

satisfy different needs on image quality and large embedding capacity, respectively.

IV. SYSTEM IMPLEMENTATION

The system output is mainly based on privacy preserving method. It will be evaluated using reversible data hiding algorithm. We propose a secure data sharing scheme for dynamic users. Key distribution is done by secure communication channels and the user can get the individual key from group manager.. A secure protocol is implemented for faster recovery and processing of data.

V. CONCULSION AND FUTURE WORK

Reversible data hiding in encrypted images is a new topic drawing attention because of the privacy-preserving requirements from cloud data management. Previous methods implement RDH in encrypted images by vacating room after encryption, as opposed to which we proposed by reserving room before encryption. Thus the data hider can benefit from the extra space emptied out in previous stage to make data hiding process effortless. The proposed method can take advantage of all traditional RDH techniques for plain images and achieve excellent performance without loss of perfect secrecy.

Furthermore, by this novel method can achieve reversibility as well as separate data extraction and greatly improvement on the quality of marked decrypted images. Real reversibility is realized that is data extraction and image recovery are free from error.

REFERENCES

1. Alireza Jolfaei and Abdolrasoul Mirghadri "Survey Image Encryption Using Salsa20", IJCSI International Journal of Computer Science Issues.
2. N. Pisarchik and M. Zanin, "Image Encryption with Chaotically Coupled Chaotic Maps," Physica D, 237,20, pp.
3. H. El-din H. Ahmed, M. K Hamdy, and O. S. Farag Allah, "Encryption quality analysis of the RC5 block cipher algorithm for digital images," Optical Engineering, vol. 45 Issue 10107003,2006.
4. Mitra, Y V. Subba Rao, and S. R. M. Prasnna, "A new image encryption approach using combinational permutation techniques," Journal of computerScience,vol.1,2006,p.127.
5. W. Lee, T. Chen and C. Chieh Lee, "Improvement of an encryption scheme for binary images," Pakistan Journal of Information and Technology.vol.2, no.2,2003,pp.191-200.
6. L. Zhi, S. A. Fen and Y. Y. Xian, "*A LSB steganography detection algorithm*", Proc. IEEE ISPIMRC, pp.2780-2783,2003.
7. A.Westfeld and A. Pfitzmann, "*Attacks on steganographic systems*,",Lecture Notes in Computer Science, 1768, pp.289-302,Springer 2001.
8. C.V. Serdean, M. Tomlinson, J. Wade, A.M. Ambroze, "*Protecting Intellectual Rights: Digital Watermarking in the wavelet domain*", IEEE Int. Workshop Trends and Recent Achievements in IT, pp.16-18,2002.
9. N. Provos and P. Honeyman, 2003. "*Hide and seek: An introduction to steganography*". IEEE Transactions on Security and Privacy, Vol.1, No.3, pp.32-44.
10. Neil F. Johnson, Zoran Duric, Sushil Jajodia, *"Information Hiding: Steganography and Watermarking: Attacks and Countermeasures", Kluwer Academic Publishers Norwell, MA, USA, pp.1*