VOL. 10, NO. 8, MAY 2015 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

LOSSLESS METHOD FOR DATA HIDING IN ENCRYPTED IMAGE

Patel Roshni[1], Aslam Durvesh[1] and Patel Urvisha[2]
[1]Department of Electronics and Communication, Parul Institute of Engineering and Technology, Limda, Vadodara, India
[2]Department of Computer Science, Mahatma Gandhi Institute of technology and Research Center, Navsari, India
E-Mail: rose.patel13188@gmail.com

ABSTRACT

The concept presents an idea to embed data in an encrypted image by using an irreversible approach of data hiding or data hiding, aimed at secretly embedding a message into the data. Massage communication over internet facing problems like data security, copyright control, data size capacity, authentication etc. A new idea is to apply reversible data hiding algorithms on encrypted images by wishing to remove the embedded data before the image decryption. The aim of this dissertation is to create a secure data hiding technology. The data hiding and image encryption are done by using two different keys. That is encryption key and the data hiding key. So the receiver who has the data hiding key can retrieve the data embedded.

Keywords: image encryption, image decryption, image recovery, reversible data hiding.

1. INTRODUCTION

In the world of internet communication, security plays an important role and owns a major regime on its stack. Now a day's data security and data integrity are challenging areas. Thus security is the key to unlock a communication box. Branch of security, which are cryptography, information hiding and watermarking etc, provides better role as they take part. As the technology keeps on changing its face with advanced features, there is necessary to get update. Usually when a new algorithm is produced or an existing algorithm is revised, intruders or hackers break the algorithm. Data security means protection of data from unauthorized users and hackers. So it is necessary to develop algorithms more efficient and unbreakable. The network security is branched into cryptography and information hiding. Information hiding contains steganography and watermarking. In cryptography, encryption of data's takes place at the transmitter and decryption at the receiver section. Thus to encrypt and decrypt same key or different keys may be used. Now extending its branches into symmetric (conventional) and asymmetric (public key) encryption. Here in the former encryption, same key is used both at the transmitter and receiver side. Coming to Steganography, which is art of concealing of data into other. It may be dated past, but again heads to more secure transmission. In order to improve the security level, combination of various techniques is handled. One such try is the Steganography over cryptography. Both the techniques provide better authentication and integrity among the users. One technique chosen under Steganography is RDH (Reversible Data Hiding). In Reversible Data Hiding, major ingredients are the cover data and the secret data. Cover data is which the secret data to be hidden, like the letter enclosed in an envelope. The other is secret or additional data. Here the overall data enclosing the cover data and secret data is called the marked cover. In Reversible Data Hiding more importance is given to the cover data, such that the user information is inscribed over it. Applications of Reversible Data Hiding are in case of military communication, in medical, in case of emergency over country, etc.

2. RELATED WORK

In [1], presented a lossless reversible data hiding technique which gives the exact recovery of the original signal and also gives exact extraction of the embedded information. And this exact recovery with lossless data is nothing but the reversible data hiding. Usually the well-known LSB method is used as the data embedding method. Reversible data hiding is a technique that is mainly used for the authentication of data like images, videos, electronic documents etc. The main application of reversible data hiding technique in Intellectual Property Rights is protection and authentication. In some application it is important to provide security and privacy during transferring data. That's why it is necessary to hide the data or to provide the data security we need new approach in internet communication.

The work in [2], presented data hiding technique using which we can extract data correctly and then original cover content can be perfectly recovered. This technique is known as reversible data hiding, lossless or distortion free technique.

Reference [3] offered a practical scheme having an encrypted image containing additional data a receiver first decrypts it according to the encryption key, and then extracts the embedded data and recovers the original image according to the data-hiding key. In this scheme the procedure of data extraction is not separable. In other words, the content of original image is revealed before payload extraction, and, if someone has the data-hiding key only but not the encryption key he is unable to extract any information from the encrypted image containing additional data.

The work in [4], gives advantages that content of the image is revealed before data extraction. If someone has the data hiding key but not the encryption key he cannot extract any information from the encrypted image containing additional data. If the receiver has only the data-hiding key, he can extract the additional data only. If

he has only the encryption key, he can decrypt the received data to obtain an image similar to the original one, but cannot extract the embedded additional data. If receiver has both the data-hiding key and the encryption key, then can extract the additional data and recover the cover image without any error if the amount of additional data is not too large.

Reference [5], presented Pseudo random sequence consists of random bits generated using the encryption key. The additional data embedded 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. Compared with the other algorithms, this system demonstrated successful accuracy in recovering the original images.

Reference [6], presented to summarize this paper, at the transmitter side an encryption is carried. Then the DFT compression is performed to the encrypted image to create the space needed to hide the secret image. In the free space provided the additional secret data is embedded using the data-hiding key. DFT thus provides efficient compression in the frequency domain. Then at the receiver side, either of the key is used independently to recover the cover image and the secret data separately. Among other compression techniques DFT operates well in the frequency domain which is best suited for audio and images. Concluding that DFT provided best compression rate and loss is a least part.

Reference [7], presented this new approach describes how we can maintain the performance after increasing the amount of payload. So after studying this technique it has been concluded that it is possible to hide large amount of data without compromising security as well as quality of the cover image. Also higher PSNR of the decrypted cover image is observed after performing encryption-decryption, data hiding and data extracting process on cover image.

3. DIFFERENT METHODS FOR IMAGE ENCRYPTION AND DECRYPTION

A. Hashing encryption

Hashing is the first encryption method, creates a unique, fixed-length signature for a message or data set. It created with hash function, and people commonly use them to compare sets of data. Since a hash is unique to a specific message, even minor changes to that message result in a dramatically different hash, there by alerting a user to potential tampering.

B. Symmetric encryption

Symmetric cryptography, also called private-key cryptography, is one of the oldest and most secure encryption methods. The term "private key" comes from the fact that the key used to encrypt and decrypt data must remain secure because anyone with access to it can read the coded messages. A sender encodes a message into cipher text using a key, and the receiver uses the same key to decode.

C. Asymmetric encryption

asymmetric or public key cryptography is potentially more secure than symmetric method of encryption. This type of cryptography uses two keys, a "private" key and a "public key" to perform encryption and decryption. The use of two keys overcomes a major weakness in symmetric key cryptography, since a single key does not need to be securely managed among multiple users.

In asymmetric cryptography, a public key is freely available to everyone and used to encrypt messages before sending them. A different, private key remains with the receiver of cipher text messages, when uses it to decrypt them. Algorithms that use public key encryption methods include RSA and Differ-Hellman.

D. AES encryption

The algorithm is flexible in supporting any combination of data and key size of 128, 192, and 256 bits. However, AES merely allows a 128 bit data length that can be divided into four basic operation blocks. These blocks operate on array of bytes and organized as a 4×4 matrix that is called the state. For full encryption, the data is passed through Nr rounds (Nr = 10, 12, 14) [4, 6]

E. Block-based transformation

The transformation technique works as follows: the original image is divided into a random number of blocks that are then shuffled within the image. The generated (or transformed) image is then fed to the Blowfish encryption algorithm. The main idea is that an image can be viewed as an arrangement of blocks. The intelligible information present in an image is due to the correlation among the image elements in a given arrangement. This perceivable information can be reduced by decreasing the correlation among the image elements using certain transformation techniques. The secret key of this approach is used to determine the seed. The seed plays a main role in building the transformation Table, which is then used to generate the transformed image with different random number of block sizes. The transformation process refers to the operation of dividing and replacing an arrangement of the original image.

4. DIFFERENT METHODS FOR DATA EMBEDDING

A. DWT watermarking

Wavelet transform is a time domain localized analysis method with the window's size fixed and forms convertible. There is quite good time differentiated rate in high frequency part of signals DWT transformed. Also there is quite good frequency differentiated rate in its low frequency part. The basic idea of discrete wavelet transform (DWT) in image process is to multi-

differentiated decompose the image into sub-image of different spatial domain and independent frequency district. Then transform the coefficient of sub-image. After the original image has been DWT transformed, it is decomposed into 4 frequency districts which is one low-frequency district (LL) and three high-frequency districts (LH, HL, HH). If the information of low-frequency district is DWT transformed, the sub-level frequency district information will be obtained. A two-dimensional image after three-times DWT decomposed can be shown as Figure-1.2. Where, L represents low-pass filter, H represents high-pass filter. An original image can be decomposed of frequency districts of HL1, LH1, HH1. The low-frequency district information also can be decomposed into sub-level frequency district information of LL2, HL2, LH2 and HH2. By doing this the original image can be decomposed for n level wavelet transformation.

B. DCT watermarking

DCT watermarking is a process of embedding information. Information embedded is imperceptible, secure and robust.

Step-1: Divides image into parts based on the visual quality of the image.

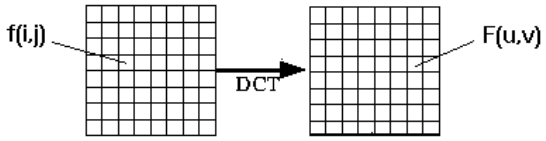


Figure-1. DCT compression method.

Step-2: Input image is N*M.
Step-3: F (i,j) = intensity of pixel in row i and column j.
Step-4: F (u,v) is DCT coefficient in DCT matrix.
Step-5: Larger amplitudes closer to F (0,0).
Step-6: Compression possible because higher order coefficients are generally negligible.

C. LSB compression method

LSB is the most basic method and used in common for creating the sparse space. The sparse space created is useful for hiding the additional payload data. This makes te works easier. In this some parameter are added into small number of encrypted pixels, and the LSB of the other encrypted pixels are compressed to create a space for accommodating additional data.

5. PROPOSED METHOD

The proposed scheme is made up of image encryption, data embedding and data-extraction/image-recovery phases. The content owner encrypts the original uncompressed image using an encryption key to produce an encrypted image. Then, the data-hider compresses the least significant bits of the encrypted image using a data-hiding key to create a sparse space to accommodate the additional data.

At the receiver side, the data embedded in the created space can be easily retrieved from the encrypted image containing additional data according to the data-hiding key. Here comprehensive combination of image encryption and data hiding compatible with lossy Compression method will be used.

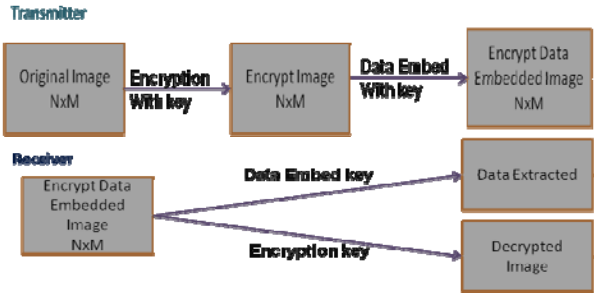


Figure-2. Block diagram.

Encryption and decryption algorithem

A. Image decryption algorithm
Step-1:
Find image size Colum and Row
Step-2:
Generate Key and mask
Keygen= Colum*Row*8
KeygenMask=Colum*Row*8
Step-3:
Putting value in mask
rvalue =0.300001;
x_N = 0;
for ind = 2 : n
x_N = 1 - 2* rvalue * rvalue; % value generation for keymask < 0
if (x_N > 0.0)
bin_x(ind-1) = 1;
end
rvalue = x_N;
end
Step-4:
Divide by 8 the mask to same size of image
KeygenMask=KeygenMask/8
Step-5:
Now apply bitxor operation between original image and KegenMask

Encrypted image = bitxor(original image,KeygenMask);

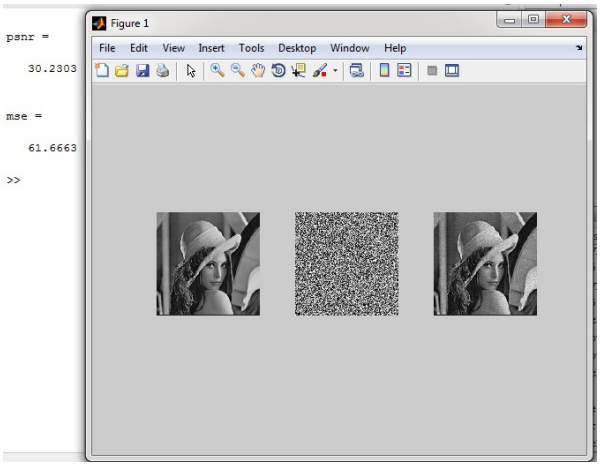
Image decryption algorithm
Step-1:
Find Encrypted Image size Colum and Row
Step-2:
If KeyGen=Colum*Row
Further Decryption Process
Else
Decryption is not done
Step-3:
Generated KeygenMask at step 2 and 3 will be use here

Step-4:
Now apply bitxor operation between Encrypted image and KegenMask

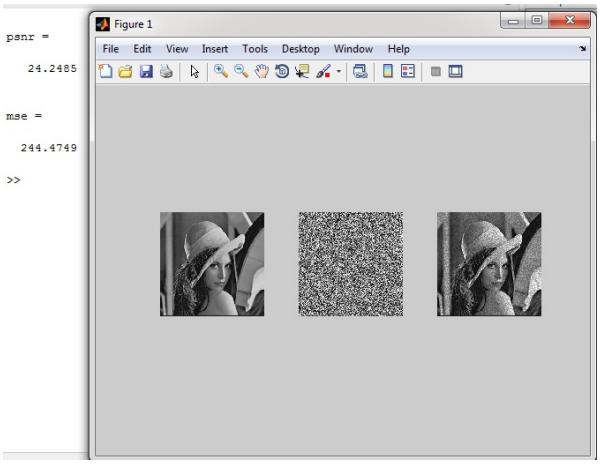
Decrypted image = bitxor(Encrypted image, KeygenMask);

6. RESULTS

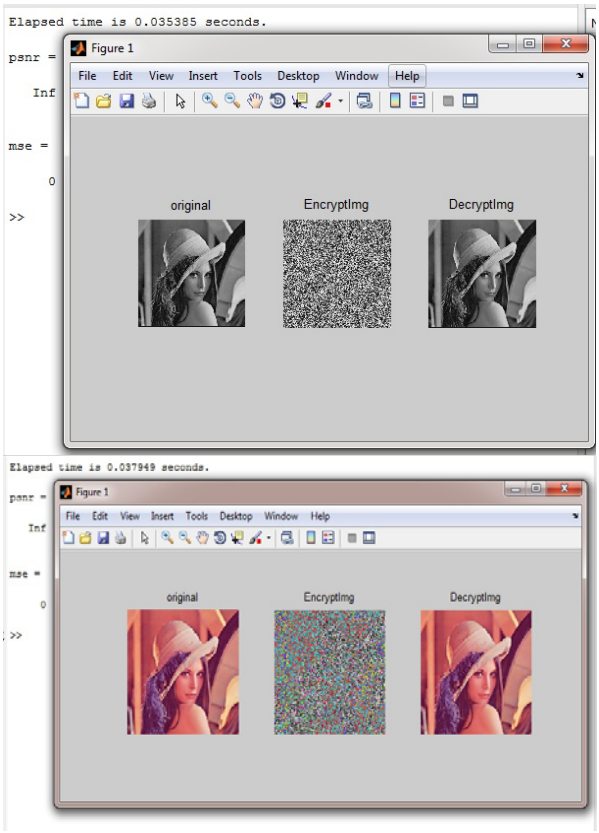
A. AES encryption and decryption



B. Block encryption and decryption



C. Proposed encryption and decryption



7. COMPARISION

Image encryption methods	PSNR	MSE
AES based algorithm	30.2303	61.663
Block-based transformation	24.2485	244.4749
Proposed method	Inf	0

8. CONCLUSIONS

Here hiding in encrypted image is proposed, which consists of image encryption, data embedding and data-extraction/image-recovery phases.

In the first phase, the content owner encrypts the original uncompressed image using an encryption key then using a data hiding key to create a sparse space to accommodate the additional data.

When the receiver has both of the keys, it can extract the data and recover the original content without any error.

In Feature we implement data hiding and extraction algorithm and combine with our system. The new technique will solve a dilemma faced by digital image users, particularly in sensitive military, legal, and medical applications for secure message transmission.

REFERENCES

[1] X Zhang, "Separable Reversible Data Hiding in Encrypted Image", IEEE transactions on information forensics and security, vol. 7, no. 2, pp. 826-832, April. 2012.

[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, March 2006.

[3] X. Zhang, "Reversible data hiding in encrypted image," IEEE Signal Process. Lett. vol. 18, no. 4, pp. 255-258, April 2011.

[4] Rini.J, 4th Semester M.Tech, Dept. of Computer Science and Information Systems FISATAngamaly, Kerala, India "Study on Separable Reversible Data Hiding in Encrypted Images" International Journal of Advancements in Research & Technology, Volume 2, Issue 12, December-2013 Copyright © 2013 SciResPub. IJOART.

[5] Vinit Agham Department of Computer Engineering R C Patel Institute of Technology, Shirpur. Dist. Dhule, Maharashtra, India. Tareek Pattewar Department of Information Technology R C Patel Institute of Technology, Shirpur. Dist. Dhule, Maharashtra, India "A Novel Approach towards Separable Reversible Data Hiding Technique" 2014 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT).

[6] Rengarajaswamy1 Assistant Professor, Department of Electronics and Communication Engineering, M.A.M School of Engineering, Trichy, Tamil Nadu "DFT Based Individual Extraction Of Steganographic Compression Of Images", IJRET February 14.

[7] Vinit Agham Department of Computer Engineering R C Patel Institute of Technology, Shirpur. Dist. Dhule, Maharashtra, India. Tareek Pattewar Department of Information Technology R C Patel Institute of Technology, Shirpur. Dist. Dhule, Maharashtra, India "A Novel Approach towards Separable Reversible Data Hiding Technique" 2014 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT).